UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In Re: Group Health Plan Litigation	Case No. 23-cv-267-JWB/DJF **CONSOLIDATED CLASS ACTION COMPLAINT**

CLASS ACTION COMPLAINT

Plaintiffs Kelly Vriezen, Sandra Tapp, and Kaye Lockrem are current patients of Group Health Plan, Inc. d/b/a HealthPartners ("Group Health Plan" or "Defendant"), who bring this class action against Defendant in their individual capacities and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions, their counsels' investigation, and upon information and belief as to all other matters, as follows:

1. Plaintiffs bring this case to address Defendant's illegal and widespread practice of disclosing Plaintiffs' and Class Members' confidential personally identifiable information (PII) and protected health information (PHI) (collectively referred to as Private Information) to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook"),

through Pixel Code ("Pixel" or "Facebook Pixel") embedded on its Website[1] and Conversions Application Programming Interface ("CAPI") residing on its Website servers.

2. Information about a person's physical and mental health—regardless of whether the information pertains to a common cold or a diagnosis of Parkinson's disease—is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage.[2]

3. Simply put, if people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems. Additionally, protecting medical information and ensuring it is kept confidential is necessary to maintain public trust in the healthcare system as a whole.

[1] Defendant owns and controls two websites, www.healthpartners.com and www.virtuwell.com (collectively Defendant's Websites or Website), which it encourages patients to use for booking medical appointments, locating physicians and treatment facilities, communicating medical symptoms, searching medical conditions and treatment options, signing up for events and classes, and more.

[2] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), available at https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited July 11, 2023) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized."); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited July 11, 2023).

4. The need for data security (and transparency) is more important than ever due to the rapidly expanding world of digital healthcare because, of all the information the average internet user communicates and transmits online, health data is some of the most valuable and controversial.[3] Health data insecurity can have serious long-term implications for individuals.

5. Despite professing to value patients' privacy and vowing to protect the confidentiality and security of their private and protected health information, healthcare entities, like Defendant, are collecting, in some instances, "ultra-sensitive personal data" about patients "ranging from those seeking information about their reproductive rights and options, those seeking information regarding their addictions and . . . those seeking mental health counseling."[4]

[3] Protected and highly sensitive medical information collected by healthcare entities includes many categories from intimate details of an individual's conditions, symptoms, diagnoses, and treatments to personally identifying information to unique codes which can identify and connect individuals to the collecting entity. *See* Molly Osberg & Dhruv Mehrotral, *The Spooky, Loosely Regulated World of Online Therapy*, Jezebel (Feb. 19, 2020), available at https://jezebel.com/the-spooky-loosely-regulated-world-of-online-therapy-1841791137 (last visited July 11, 2023).

[4] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, Reveal (June 15, 2022), available at https://revealnews.org/article/facebook-data-abortion-crisis-pregnancy-center/ (noting that such "personal data can be used in a number of ways. The centers can deliver targeted advertising, on Facebook or elsewhere, aimed at deterring an individual from getting an abortion. It can be used to build anti-abortion ad campaigns – and spread misinformation about reproductive health – targeted at people with similar demographics and interests. And, in the worst-case scenario now contemplated by privacy experts, that digital trail might even be used as evidence against abortion seekers in states where the procedure is outlawed") (last visited July 11, 2023).

6. And, while mobile health options have been celebrated as a way to expand treatment options, the tangible, real-world implications and potential for abuse is staggering:

> [T]he sensitive information people share during treatment for substance use disorders could easily impact their employment status, ability to get a home, custody of their children, and even their freedom. Health care providers and lawmakers recognized long ago that the potential threat of losing so much would deter people from getting life-saving help and set up strict laws to protect those who do seek treatment. ***Now, experts worry that data collected on telehealth sites could bring about the harm [the law] was designed to prevent and more, even inadvertently***.[5]

7. Recognizing these incontrovertible facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how health care providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

8. Healthcare organizations regulated under HIPAA may use third-party tracking tools, such as Google Analytics or the Facebook Pixel, only in a limited way to perform analysis on data that is key to their operations:

> To be sure, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has made clear, in a recent bulletin

[5] *Id.* (emphasis added).

> entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule: Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individual HIPAA-compliant authorizations, would constitute impermissible disclosures.***[6]

9. In addition, Minnesota law provides that all medical records must be treated as confidential unless disclosure falls within the exceptions listed in the Minnesota Health Records Act. *See* Minn. Stat. § 144.293, subd. 1. None of the exceptions apply based on the facts set forth in this Consolidated Class Action Complaint.[7]

10. Further, Minnesota's Patient Bill of Rights states "patients shall be assured confidential treatment of their personal and medical records, and may approve or refuse their release to any individual outside of the facility." Minn. Stat. § 144.651 subd. 16.

11. Defendant devotes a section of its Website to a "Online Patient Services System" (formerly known as MyChart) ("Online Patient Services")[8] which encourages

[6] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept. of Health & Hum. Servs. (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited May 10, 2023) (emphasis added).

[7] *See* Minn. Stat. 144.293, subd. 5 (stating potential exceptions to consent requirement—*i.e.*, healthcare provider may disclose medical records with patient consent, for medical emergency, to other providers within scope of current treatment, to healthcare facilities, for patient returning to healthcare facility unable to provide consent, and to another provider for the purpose of diagnosing or treating deceased patient's surviving child).

[8] *Online Patient Services Terms and Conditions*, Health Partners, https://www.healthpartners.com/hp/legal-notices/terms/online/index.html (last visited July 9, 2023).

patients to sign up to access Online Patient Services so that they can more conveniently book appointments and schedule visits, review their health records and test results, pay bills, communicate with service providers, request prescription refills, and complete medical forms virtually and remotely.

12. Upon information and belief, the Online Patient Services portal is a software system designed and licensed to Defendant by Epic Software Systems ("Epic"). Epic is a privately owned health care software company that provides services to 250 million patients, including two-thirds of the U.S. population.

13. Epic's MyChart software system was designed to permit licensees—such as Defendant—to deploy "custom analytics scripts" within MyChart, including, for example, the Facebook Pixel or Google Analytics, which call for the transmission of personally identifiable information, including medical and health-related information, and communications to third parties.[9]

14. As a result, hospitals that use analytics tools like the Facebook Pixel or Google Analytics—including Defendant—may also be using those tools on their Online Patient Services login page and inside password protected portions of the Online Patient Services patient portal.

[9] *See* T. Feathers, et al., *Pixel Hunt: Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-isreceiving-sensitive-medical-information-from-hospital-websites (last visited July 11, 2023).

15. Defendant's Website encourages patients to use the Online Patient Services portal by promoting the service and advertising its functionality.

16. Plaintiffs and other Class Members who used Defendant's Website reasonably believed they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiffs and Class Members, however, Defendant had embedded the Pixel into its Website, surreptitiously forcing Plaintiffs and Class Members to transmit their Private Information to Facebook without consent.

17. Operating as designed and as implemented by Defendant, the Pixel causes Plaintiffs' and Class Members' Private Information to be unlawfully disclosed to Facebook alongside the individual's unique and persistent Facebook ID ("FID"), thereby linking their Private Information to their specific profile and other data.[10]

18. A "pixel" in this context is a piece of code that "tracks the people and [the] type of actions they take"[11] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view,

[10] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." "Cookies help inform websites about the user, enabling the websites to personalize the user experience." *What are Cookies?*, CloudFlare, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited July 11, 2023).

[11] *Retargeting*, Facebook, https://www.facebook.com/business/goals/retargeting (last visited July 11, 2023).

and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

19. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Facebook Pixel is thus customizable and programmable, meaning that the website owner controls which of its webpages contain the Pixel and which events are tracked and transmitted to Facebook.

20. When a website user visits a webpage containing a Pixel, their device is commandeered, and their communications are surreptitiously duplicated and transmitted to third parties. Stated differently, Defendant's Website and Pixel purposely altered patients' web browsers, forcing them to duplicate and redirect communications to third-party web servers without their authorization or knowledge.

21. The information sent to third parties included the Private Information that Plaintiffs and Class Members submitted to Defendant's Website related to their past, present, or future health conditions, including, for example, the type and date of a medical appointment and selected physician. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care as well as the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or addiction.

22. Simply put, by installing the Facebook Pixel into its Website, Defendant effectively planted a bug on Plaintiffs' and Class Members' web browsers and compelled them to disclose their communications with Defendant to Facebook.

23. In addition to the Pixel, Defendant also has CAPI on its Website servers.[12]

24. Unlike the Facebook Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[13, 14] Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[15]

[12] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See How to Implement Facebook Conversions API*, Fetch & Funnel, https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited July 11, 2023).

[13] *What is the Facebook Conversions API and How to Use* it, Revealbot, https://revealbot.com/blog/facebook-conversions-api/ (last visited July 11, 2023).

[14] "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel…. This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *Conversions API*, Meta for Developers, https://developers.facebook.com/docs/marketing-api/conversions-api (last visited July 11, 2023).

[15] *About Conversions API*, Meta Business Help Center, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited July 11, 2023).

25. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

26. Defendant utilized the Pixel and CAPI data for marketing purposes in an effort to bolster its profits. The Facebook Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

27. The information disclosed in this way by Defendant allows a third party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who geotarget Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Facebook Pixel and CAPI.

28. The Office for Civil Rights (OCR) at HHS has issued a Bulletin to specifically highlight and address the obligations of HIPAA covered entities and business associates under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies.[16] The Bulletin expressly provides that

[16] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept. of Health & Hum. Servs. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

these "entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules." In other words, HHS has expressly stated that covered or regulated entities that implement the Facebook Pixel as Defendant has are in violation of HIPAA Rules.

29. The HHS Bulletin further warns that:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [17]

30. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party – let alone Facebook, which has a sordid history of privacy violations, in pursuit of ever-increasing advertising revenue – without the patients' consent. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook.

[17] *Id*. (emphasis in the original).

31. Despite willfully and intentionally incorporating the Facebook Pixel and CAPI into its Website and servers, Defendant has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to Facebook as they communicated with their healthcare provider via the Website or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.

32. In the alternative, Defendant negligently enabled its Website and servers to contain the Pixel and CAPI without disclosing its existence to its patients, and thus unlawfully and negligently tracked and transmitted Plaintiffs' and Class Members' Private Information to Facebook.

33. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, inter alia: (i) failing to adequately review its marketing programs and web-based technology to ensure its Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Facebook Pixels; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to

design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

34. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) loss of benefit of the bargain, (iii) diminution of value of the Private Information, (iv) statutory damages, and (v) the continued and ongoing risk to their Private Information.

35. Plaintiffs seek to remedy these harms and bring causes of action for (1) violations of the Minnesota Health Records Act, Minn. Stat. § 144.291, *et seq*.; (2) invasion of privacy; (3) breach of implied contract; (4) unjust enrichment; (5) breach of fiduciary duty; (6) breach of confidence; (7) negligence; (8) violations of ECPA, 18 U.S.C. § 2511(3)(a) -unauthorized interception, use, and disclosure; and (9) violations of Minnesota's Unfair and Deceptive Trade Practices Act (Minn. Stat. §325D.43-48).

PARTIES

Plaintiff Kelly Vriezen

36. Plaintiff Vriezen is a natural person and citizen of Minnesota where she intends to remain. On numerous occasions, Plaintiff Vriezen accessed Defendant's Website on her mobile device and/or computer. Plaintiff Vriezen used the Website to find and obtain medical treatment. Pursuant to the systematic process described in this Complaint, Plaintiff Vriezen's Private Information was disclosed to Facebook, and this data included her Private Information, Defendant intercepted and/or assisted these interceptions without Plaintiff's knowledge, consent, or express written authorization. By failing to receive the

requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Vriezen's Private Information.

37. Plaintiff Vriezen has been Defendant's patient and received healthcare services since 2017 at one of the hospitals in Defendant's network, and she has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

38. Plaintiff Vriezen has been using Defendant's Website, including the Virtuwell Webpage, since 2017.

39. Plaintiff Vriezen has been a Facebook user since 2008.

40. Plaintiff Vriezen accessed Defendant's Website, including the Virtuwell Webpage, to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

41. Plaintiff Vriezen used and continues to use Defendant's Website on a regular basis, including the Virtuwell Webpage, to conduct the following activities: communicate private health information with her healthcare provider, search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

42. For example, Plaintiff Vriezen has searched Defendant's Website for symptoms and treatment pertaining to her specific personal medical conditions.[18]

[18] To the extent the Court so desires, Plaintiff Vriezen is willing to disclose the precise medical conditions and treatment she communicated to Defendant via Defendant's Website.

43. Based on the presence of the Pixel on its Websites during the times that Plaintiff Vriezen submitted her personal medical information to Defendant, Defendant unlawfully tracked and unlawfully transmitted her Private Information to Facebook.

44. This allegation is confirmed *infra* at paragraphs ¶¶186-187 which demonstrate, alongside relevant images taken from Plaintiff Vriezen's Facebook account, that her communications with Defendant via its Website were indeed transmitted and divulged to Facebook beginning, at a minimum, in May 2021 when she used Defendant's Website.

45. As Defendant's patient, Plaintiff Vriezen reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted or intercepted by a third party.

46. Plaintiff Vriezen never observed and/or witnessed any disclaimer on Defendant's Website that explicitly stated that her communications on Defendant's Website would be transmitted to Facebook.

47. As Defendant's patient, Plaintiff Vriezen reasonably expected Defendant would safeguard any Private Information she communicated to Defendant via its Website. But for her status as Defendant's patient, Plaintiff Vriezen would not have disclosed her Private Information to Defendant.

48. During her time as Defendant's patient, Plaintiff Vriezen never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

49. Despite her status as Defendant's patient, Defendant's Website routinely provided Facebook with Plaintiff Vriezen's FIDs, IP addresses, and/or device IDs or other information she input into Defendant's Website, like medical conditions, associated symptoms, and searches for doctors. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[19] Plaintiff Vriezen's and Class Members' identities could be easily determined based on the FID, IP address, and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

50. After intercepting and collecting Plaintiff Vriezen's information, Facebook processed it, analyzed it, and assimilated it into datasets like Core Audiences and Custom Audiences. Because Plaintiff Vriezen is a Facebook user, Facebook associated the information that it collected from Defendant's Website to Plaintiff Vriezen's FID that identified her name and Facebook profile, i.e., her real-world identity. Plaintiff Vriezen's Facebook Profile ID is linked to her Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because Plaintiff Vriezen's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

[19] *Supra* n.16.

51. In sum, Defendant's Pixel transmitted Plaintiff Vriezen's highly sensitive communications and Private Information to Facebook, including communications that contained Private and confidential information, without Plaintiff Vriezen's knowledge, consent, or express written authorization.

52. Defendant breached Plaintiff Vriezen's right to privacy and unlawfully disclosed her Private Information to Facebook. Specifically, Plaintiff Vriezen had a reasonable expectation of privacy, based on her status as Defendant's patient, that Defendant would not disclose her Private Information to third parties.

53. Defendant did not inform Plaintiff Vriezen that it shared her Private Information with Facebook.

54. By doing so without Plaintiff Vriezen's consent, Defendant breached Plaintiff Vriezen's right to privacy and unlawfully disclosed Plaintiff Vriezen's Private Information.

55. Upon information and belief, as a "redundant" measure to ensure Plaintiff Vriezen's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like CAPI to send Plaintiff Vriezen's Private Information from electronic storage on Defendant's server directly to Facebook.

56. Plaintiff Vriezen suffered injuries in the form of (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to her Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff Vriezen's medical

conditions and other confidential information she communicated to Defendant via the Website.

57. As a result of Defendant's surreptitious use of the Pixel and CAPI on its Website, Plaintiff Vriezen has suffered mental anguish, stress, and anxiety from the unlawful disclosure of her Private Information to Facebook.

58. Plaintiff Vriezen has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

Plaintiff Kaye Lockrem

59. Plaintiff Lockrem is a natural person and citizen of Minnesota where she intends to remain. On numerous occasions, Plaintiff Lockrem accessed Defendant's Website on her mobile device and/or computer. Plaintiff Lockrem used the Website to find and obtain medical treatment. Pursuant to the systematic process described in this Complaint, Plaintiff Lockrem's Private Information was disclosed to Facebook, and this data included her Private Information. Defendant intercepted and/or assisted these interceptions without Plaintiff Lockrem's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Lockrem's Private Information.

60. Plaintiff Lockrem has been Defendant's patient and received healthcare services since 2012 at one of the hospitals in Defendant's network, and she has used

Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

61. Plaintiff Lockrem has been using Defendant's Website, including the Virtuwell Webpage since 2013.

62. Plaintiff Lockrem has been a Facebook user since 2012.

63. Plaintiff Lockrem accessed Defendant's Website, including the Virtuwell Webpage, to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

64. Plaintiff Lockrem used and continues to use Defendant's Websites on a regular basis, including the Virtuwell Webpage, to conduct the following activities: communicate private health information, search for physicians, review medical bills, and search symptoms and medical conditions regarding her personal medical treatment.

65. For example, as recently as July 5, 2023, Plaintiff Lockrem searched Defendant's Websites for symptoms and treatment pertaining to a specific medical condition.[20]

66. Based on the presence of the Pixel on its Websites during the times that Plaintiff Lockrem submitted her personal medical information to Defendant, Plaintiff Lockrem alleges that Defendant unlawfully tracked and unlawfully transmitted her Private Information to Facebook.

[20] *See supra* n.18.

67. As Defendant's patient, Plaintiff Lockrem reasonably expected that any online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted or intercepted by a third party.

68. Plaintiff Lockrem never observed and/or witnessed any disclaimer on Defendant's Website that explicitly stated that her communications on Defendant's Website would be transmitted to Facebook.

69. As Defendant's patient, Plaintiff Lockrem reasonably expected Defendant would safeguard any Private Information she communicated to Defendant via its Website. But for her status as Defendant's patient, Plaintiff Lockrem would not have disclosed her Private Information to Defendant.

70. During her time as Defendant's patient, Plaintiff Lockrem never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

71. Despite her status as Defendant's patient, Defendant's Website routinely provided Facebook with Plaintiff Lockrem's FIDs, IP addresses, and/or device IDs or other information she input into Defendant's Website, like medical conditions, associated symptoms, and searches for doctors. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[21] Plaintiff Lockrem's and Class Members' identities could be easily determined based on the FID, IP

[21] *See supra* n.16.

address, and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

72. After intercepting and collecting Plaintiff Lockrem's information, Facebook processed it, analyzed it, and assimilated it into datasets like Core Audiences and Custom Audiences. Because Plaintiff Lockrem is a Facebook user, Facebook associated the information that it collected from Defendant's Website to Plaintiff Lockrem's FID that identified her name and Facebook profile, i.e., her real-world identity. Plaintiff Lockrem's Facebook Profile ID is linked to her Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because Plaintiff Lockrem's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

73. In sum, Defendant's Pixel transmitted Plaintiff Lockrem's highly sensitive communications and Private Information to Facebook, including communications that contained Private and confidential information, without Plaintiff Lockrem's knowledge, consent, or express written authorization.

74. Defendant did not inform Plaintiff Lockrem that it shared her Private Information with Facebook.

75. By doing so without Plaintiff Lockrem's consent, Defendant breached Plaintiff Lockrem's right to privacy and unlawfully disclosed Plaintiff Lockrem's Private Information.

76. Upon information and belief, as a "redundant" measure to ensure Plaintiff Lockrem's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like CAPI to send Plaintiff Lockrem's and Class Members' Private Information from electronic storage on Defendant's server directly to Facebook.

77. Plaintiff Lockrem suffered injuries in the form of (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to her Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff Lockrem's medical conditions and other confidential information she communicated to Defendant via the Website.

78. As a result of Defendant's surreptitious use of the Pixel and CAPI on its Website, Plaintiff Lockrem has suffered mental anguish, stress, and anxiety from the unlawful disclosure of her Private Information to Facebook.

79. Plaintiff Lockrem has a continuing interesting in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

Plaintiff Sandra Tapp

80. Plaintiff Tapp is a natural person and citizen of Minnesota where she intends to remain. On numerous occasions, Plaintiff Tapp accessed Defendant's Website on her mobile device and/or computer. Plaintiff Tapp used the Website to find and obtain medical treatment. Pursuant to the systematic process described in this Complaint, Plaintiff Tapp's Private Information was disclosed to Facebook, and this data included her Private Information, and related confidential information. Defendant intercepted and/or assisted these interceptions without Plaintiff Tapp's knowledge, consent, or express written authorization. By failing to receive the requisite consent, Defendant breached confidentiality and unlawfully disclosed Plaintiff Tapp's Private Information.

81. Plaintiff Tapp has been Defendant's patient and received healthcare services since 2012 at one of the hospitals in Defendant's network, and she has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

82. Plaintiff Tapp has been using Defendant's Website, including the Virtuwell Webpage, since 2007.

83. Plaintiff Tapp has been a Facebook user since 2009.

84. Plaintiff Tapp accessed Defendant's Website, including the Virtuwell Webpage, to receive healthcare services from Defendant or Defendant's affiliates, at Defendant's direction, and with Defendant's encouragement.

85. Plaintiff Tapp used and continues to use Defendant's Websites on a regular basis, including the Virtuwell Webpage, to conduct the following activities: communicate

health information, schedule appointments, and correspond with her healthcare provider regarding her personal medical treatment.

86. Based on the presence of the Pixel on its Websites during the times that Plaintiff Tapp submitted her personal medical information to Defendant, Plaintiff Tapp alleges that Defendant unlawfully tracked and unlawfully transmitted her Private Information to Facebook.

87. As Defendant's patient, Plaintiff Tapp reasonably expected that any online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted or intercepted by a third party. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Tapp would not have disclosed her Private Information to Defendant.

88. During her time as a patient, Plaintiff Tapp never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

89. As Defendant's patient, Plaintiff Tapp reasonably expected that her online communications with Defendant were solely between herself and Defendant and that such communications would not be transmitted or intercepted by a third party.

90. Plaintiff Tapp never observed and/or witnessed any disclaimer on Defendant's Website that explicitly stated that her communications on Defendant's Website would be transmitted to Facebook.

91. As Defendant's patient, Plaintiff Tapp reasonably expected Defendant would safeguard any Private Information she communicated to Defendant via its Website. But for her status as Defendant's patient, Plaintiffs Tapp would not have disclosed her Private Information to Defendant.

92. During her time as a patient, Plaintiff Tapp never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook, to access or interpret such information.

93. Despite her status as Defendant's patient, Defendant's Website routinely provided Facebook with Plaintiff Tapp's FIDs, IP addresses, and/or device IDs or other information she input into Defendant's Website, like medical conditions, associated symptoms, and searches for doctors. This is precisely the type of information that HIPAA requires healthcare providers to anonymize to protect the privacy of patients.[22] Plaintiff Tapp's identity could be easily determined based on the FID, IP address, and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

94. After intercepting and collecting Plaintiff Tapp's information, Facebook processed it, analyzed it, and assimilated it into datasets like Core Audiences and Custom Audiences. Because Plaintiff Tapp is a Facebook user, Facebook associated the information that it collected from Defendant's Website to Plaintiff Tapp's FID that identified her name and Facebook profile, i.e., her real-world identity. Plaintiff Tapp's Facebook Profile ID is linked to her Facebook profile, which generally contains a wide

[22] *See supra* n.16.

range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the Plaintiff Tapp's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

95. In sum, Defendant's Pixel transmitted Plaintiff Tapp's highly sensitive communications and Private Information to Facebook, including communications that contained Private and confidential information, without Plaintiff Tapp's knowledge, consent, or express written authorization.

96. Defendant breached Plaintiff Tapp's right to privacy and unlawfully disclosed her Private Information to Facebook. Specifically, Plaintiff Tapp had a reasonable expectation of privacy, based on her status as Defendant's patient, that Defendant would not disclose her Private Information to third parties.

97. Defendant did not inform Plaintiff Tapp that it shared her Private Information with Facebook.

98. By doing so without Plaintiff Tapp's consent, Defendant breached Plaintiff Tapp's right to privacy and unlawfully disclosed Plaintiff Tapp's Private Information.

99. Upon information and belief, as a "redundant" measure to ensure Plaintiff Tapp's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff

Tapp's Private Information from electronic storage on Defendant's server directly to Facebook.

100. Plaintiff Tapp suffered injuries in the form of (i) invasion of privacy; (ii) diminution of value of the Private Information; (iii) statutory damages; (iv) the continued and ongoing risk to her Private Information; and (v) the continued and ongoing risk of harassment, spam, and targeted advertisements specific to Plaintiff Tapp's medical conditions and other confidential information she communicated to Defendant via the Website.

101. As a result of Defendant's surreptitious use of the Pixel and CAPI on its Website, Plaintiff Tapp has suffered mental anguish, stress, and anxiety from the unlawful disclosure of her Private Information to Facebook.

102. Plaintiff Tapp has a continuing interesting in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure.

Defendant Group Health, Inc. d/b/a HealthPartners

103. Defendant Group Health, Inc. d/b/a HealthPartners is headquartered at 8170 33rd Ave., S. Bloomington, MN 55425. Defendant is an integrated health care organization providing healthcare services and health plan financing and administration, and it was founded in 1957 as a cooperative. Defendant is the largest consumer governed nonprofit health care organization in the nation – serving more than 1.8 million medical and dental health plan members nationwide. Its care system includes a multi-specialty group practice

of more than 1,800 physicians that serves more than 1.2 million patients. HealthPartners employs over 26,000 people, "all working together to deliver the HealthPartners mission."[23]

104. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d and 45 C.F.R. Part 160-45 C.F.R. Part 162, and 45 C.F.R. Part 164 (HIPAA))

JURISDICTION & VENUE

105. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant.[24]

106. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges question of federal laws under the ECPA (28 U.S.C. § 2511, *et seq.*).

107. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

[23] *About*, HealthPartners, https://www.healthpartners.com/about/ (last visited July 11, 2023).

[24] Defendant operates and caters to residents in Wisconsin, including, but not limited to, the Hudson Hospital Clinic, Westfields Hospital, and the Amery Hospital & Clinic.

108. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

A. Background: Underlying Technology Employed by Defendant for the Purpose of Disclosing Plaintiffs' and Class Members' Private Information to Facebook.

109. Defendant uses the Website to connect Plaintiffs and Class Members to Defendant's digital healthcare platforms with the goal of increasing profitability.

110. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendant purposely installed the Pixel and CAPI tools on many of its webpages within its Website and on its servers and programmed those webpages and servers. In doing so, Defendant surreptitiously shared patients' private and protected communications with Facebook, including communications that contain Plaintiffs' and Class Members' Private Information.

111. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows:

i. Facebook's Business Tools and the Pixel.

112. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[25]

[25] *Meta Reports Fourth Quarter and Full Year 2021 Results*, Meta Investor Relations, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited July 11, 2023).

113. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilizes its "Business Tools" to gather, identify, target, and market products and services to individuals.

114. Facebook's Business Tools, including the Pixel and CAPI, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

115. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, that webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[26] Advertisers, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[27]

116. One such Business Tool is the Pixel that "tracks the people and type of actions they take."[28] When a user accesses a webpage that is hosting the Pixel, the

[26] *Specifications for Meta Pixel Standard Events*, Meta Business Help Center, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (last visited July 11, 2023); *see Meta Pixel, Accurate Event Tracking, Advanced*, Meta for Developers, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also Best Practices for Meta Pixel Setup*, Meta Business Help Center, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; *App Events API*, Meta for Developers, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited July 11, 2023).

[27] *About Standard and Custom Website Events*, Meta Business Help Center, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* Facebook, *App Events API*, *supra*.

[28] *Retargeting*, Meta Business Help Center, https://www.facebook.com/business/goals/retargeting (last visited July 11, 2023).

communications with the host webpage are instantaneously and surreptitiously duplicated and sent to Facebook's servers—traveling from the user's browser to Facebook's server.

117. Notably, this transmission only occurs on webpages that contain the Pixel. Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via the Pixel but for Defendant's decisions to install the Pixel on its Website.

118. Similarly, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via CAPI but for Defendant's decision to install and implement that tool.

119. By installing and implementing both tools, Defendant caused Plaintiffs' and Class Members' communications to be intercepted and transmitted to Facebook via the Pixel, and it caused a second improper disclosure of that information via CAPI.

ii. Defendant's method of transmitting Plaintiffs' and Class Members' Private Information via the Pixel and/or CAPI i.e., the interplay between HTTP Requests and Responses, Source Code, and the Pixel

120. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

121. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

122. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.

123. To understand this terminology, HTTP Request, Cookies and HTTP Response are defined as:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF for filing a motion to a court).
- **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP

Responses may consist of a web page, another kind of file, text information, or error codes, among other data.[29]

124. When an individual visits Defendant's Website, an HTTP Request is sent from that individual's web browser to Defendant's servers that essentially asks Defendant's Website to retrieve certain information (such as Defendant's "Make an Appointment" page). The HTTP Response from Defendant's servers sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website.

125. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

126. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to HealthPartner's or Virtuwell's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is, in essence, handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-

[29] One browsing session may consist of hundreds or thousands of individual HTTP Requests and HTTP Responses.

based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook.

127. Separate from the Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as they move around the internet – whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendant's Website, a unique id is sent to Facebook along with the intercepted communication that allows Facebook to identify the patient associated with the Private Information it has intercepted.

128. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third parties bent on gathering Private Information, like Facebook, implement workarounds that savvy users cannot evade. Facebook's workaround, for example, is called CAPI.

129. CAPI is an effective workaround because it does the transmission from the website host's own servers and does not rely on the user's web browsers.

130. CAPI "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."[30] Thus, the communications between patients and

[30] *Prepare your Business to Use the Conversions API*, Meta Business Help Center, https://www.facebook.com/business/help/1295064530841207?id=818859032317965 (last visited July 11, 2023).

Defendant, which by practical necessity require use of Defendant's Website, are received by Defendant and stored on its server before CAPI sends the Private Information contained in those communications directly to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

131. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like CAPI without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[31] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the CAPI workaround.

132. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner.

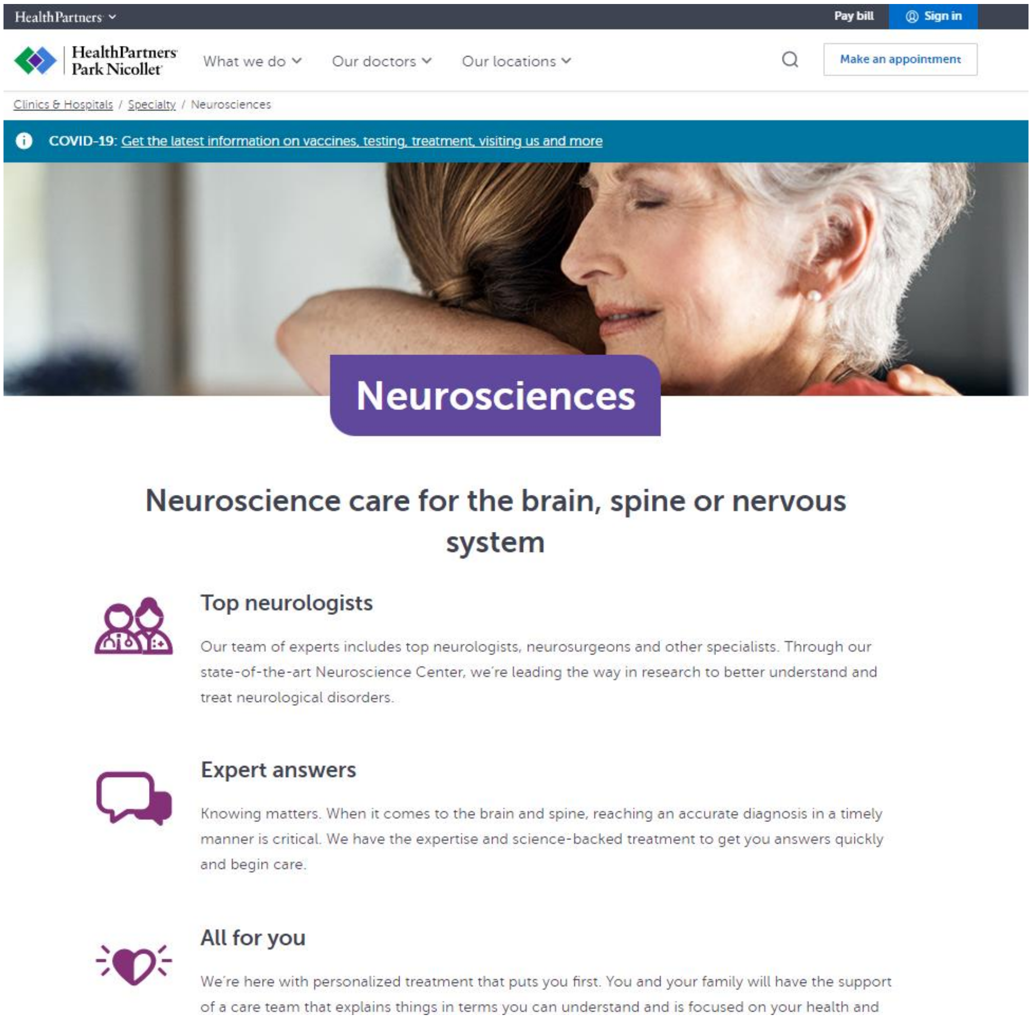
133. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device,

[31] *See Best Practices for Conversions API*, Meta Business Help Center, https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited July 11, 2023).

causing the device to contemporaneously and invisibly re-direct the user's communications to third parties.

134. In this case, Defendant employed the Pixel and/or CAPI to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to Facebook.

135. For example, when patients visit www.healthpartners.com/care/specialty/ and selects "Neuroscience," the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage as depicted below.



COVID-19: Get the latest information on vaccines, testing, treatment, visiting us and more

Neurosciences

Neuroscience care for the brain, spine or nervous system

Top neurologists

Our team of experts includes top neurologists, neurosurgeons and other specialists. Through our state-of-the-art Neuroscience Center, we're leading the way in research to better understand and treat neurological disorders.

Expert answers

Knowing matters. When it comes to the brain and spine, reaching an accurate diagnosis in a timely manner is critical. We have the expertise and science-backed treatment to get you answers quickly and begin care.

All for you

We're here with personalized treatment that puts you first. You and your family will have the support of a care team that explains things in terms you can understand and is focused on your health and

Figure 1 Image taken from https://www.healthpartners.com/care/specialty/neuroscience/.

136. The patient visiting this particular web page only sees the Markup, not the Defendant's Source Code or underlying HTTP Requests and Responses.

137. The Facebook Pixel is embedded in Defendant's Source Code contained in its HTTP Response. The Pixel, programmed to automatically track and transmit the patient's communications with Defendant's Website to Facebook, executes instructions

that effectively open a hidden spying window into the patient's browser through which Facebook can intercept the visitor's data, actions, and communications with Defendant.[32]

138. Defendant's Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Facebook. These transmissions occur contemporaneously, invisibly, and without the patient's knowledge.

139. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" its patients' computing devices, allowing Facebook and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

140. Consequently, when Plaintiffs and Class Members visit Defendant's website and communicate their Private Information, including, but not limited to, selected physician's name and specialty, specific button/menu selections, and content typed into free text boxes (such as searches for symptoms or treatment options), it is simultaneously intercepted and transmitted to Facebook.

[32] When used in the context of a screen or visual display, a "pixel" is the smallest unit in such a digital display. An image or video on a device's screen can be made up of millions of individual pixels. The Facebook Pixel is a tiny image file that is so small as to be invisible to website users. It is purposefully designed and camouflaged in this manner so that website users remain unaware of it.

B. Defendant's Pixel and/or CAPI Tracking Practices caused Plaintiffs' and Class Members' Private Information to be sent to Facebook.

141. Defendant utilizes Facebook's Business Tools and intentionally installed the Pixel and Conversions API on its Website to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.[33]

142. Defendant's Pixel has its own unique identifier (represented as id= 1113456592041476) that is contained on Defendant's Website.

143. The Pixel allows Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.[34] However, Defendant's Website does not rely on the Pixel in order to function.

144. While seeking and using Defendant's services as a medical provider, Plaintiffs and Class Members communicated their Private Information to Defendant via its Website.

145. Plaintiffs and Class Members were not aware that their Private Information would be shared with Facebook as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

[33] *Id.*

[34] *Id.*

146. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to Facebook, nor did they intend for Facebook to be a party to their communications with Defendant.

147. Defendant's Pixel and CAPI sent non-public Private Information to Facebook, including, but not limited to Plaintiffs' and Class Members': (1) status as medical patients; (2) health conditions; (3) sought treatment or therapies; (4) appointment requests and appointment booking information; (5) registration or enrollment in medical classes (such as breastfeeding courses); (6) locations or facilities where treatment is sought; (7) which webpages were viewed; and (8) phrases entered and search queries conducted via the general search bar.

148. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside the Plaintiffs' and Class Members' Facebook ID (c_user cookie or "FID"), thereby allowing individual patient's communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.[35]

149. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's

[35] Defendant's Website tracks and transmits data via first-party and third-party cookies. The c_user cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is comprised by a unique and persistent set of numbers.

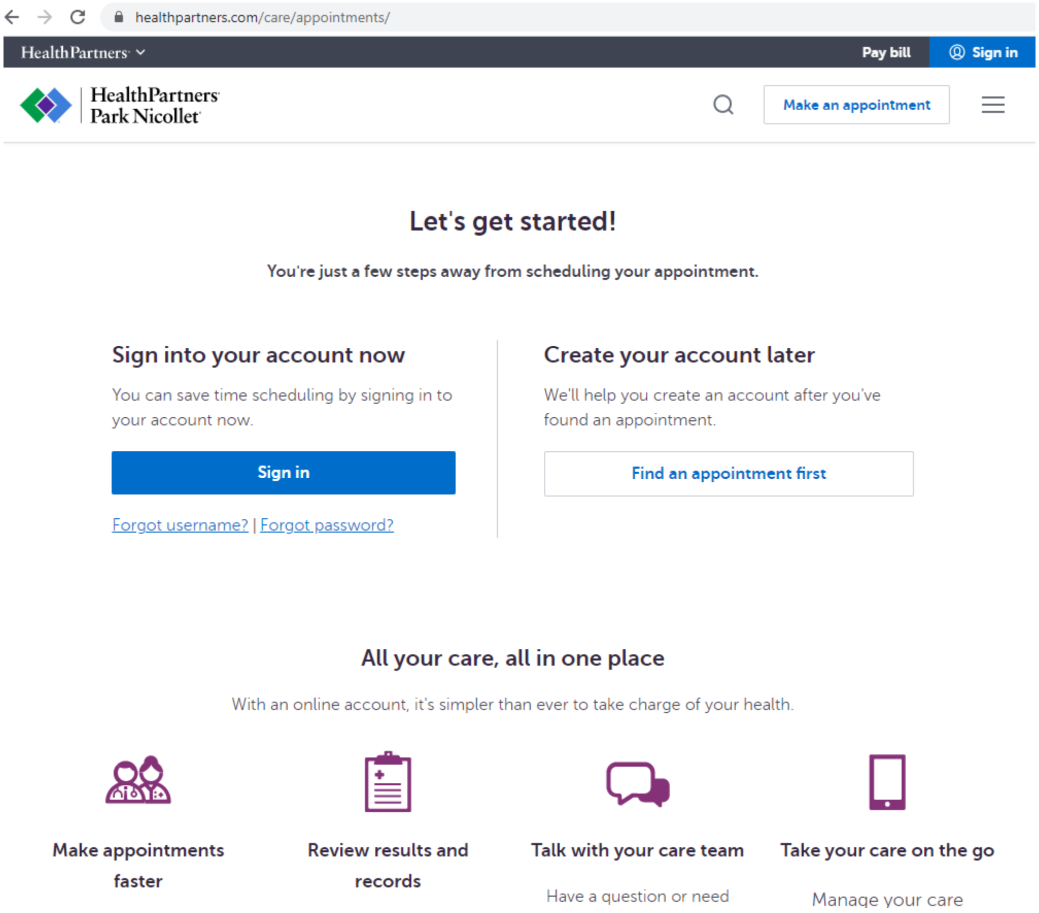
Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to locate, access, and view the user's corresponding Facebook profile quickly and easily.

150. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Facebook Pixel and CAPI) that surreptitiously tracked, recorded, and disclosed confidential communications and Private Information; (2) disclosed patients' protected information to Facebook—an unauthorized third-party; and (3) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

i. Defendant's Pixel Disseminates Patient Information via www.HealthPartners.com.

151. An example illustrates the point. If a patient uses www.healthpartners.com to book an appointment with a gynecologist for the purpose of obtaining birth control, Defendant's Webpage directs them to a series of screens that ask the patient to communicate additional information. Unbeknownst to the patient, each and every communication is sent to Facebook via Defendant's Pixel, as evidenced by the images below.

152. In order to book an appointment, the user visits www.healthpartners.com/care/appointments and clicks the "Find an appointment first" button.



healthpartners.com/care/appointments/
HealthPartners
Pay bill
Sign in
HealthPartners Park Nicollet
Make an appointment

Let's get started!

You're just a few steps away from scheduling your appointment.

Sign into your account now

You can save time scheduling by signing in to your account now.

Sign in
Forgot username? | Forgot password?

Create your account later

We'll help you create an account after you've found an appointment.

Find an appointment first

All your care, all in one place

With an online account, it's simpler than ever to take charge of your health.

Make appointments faster

Review results and records

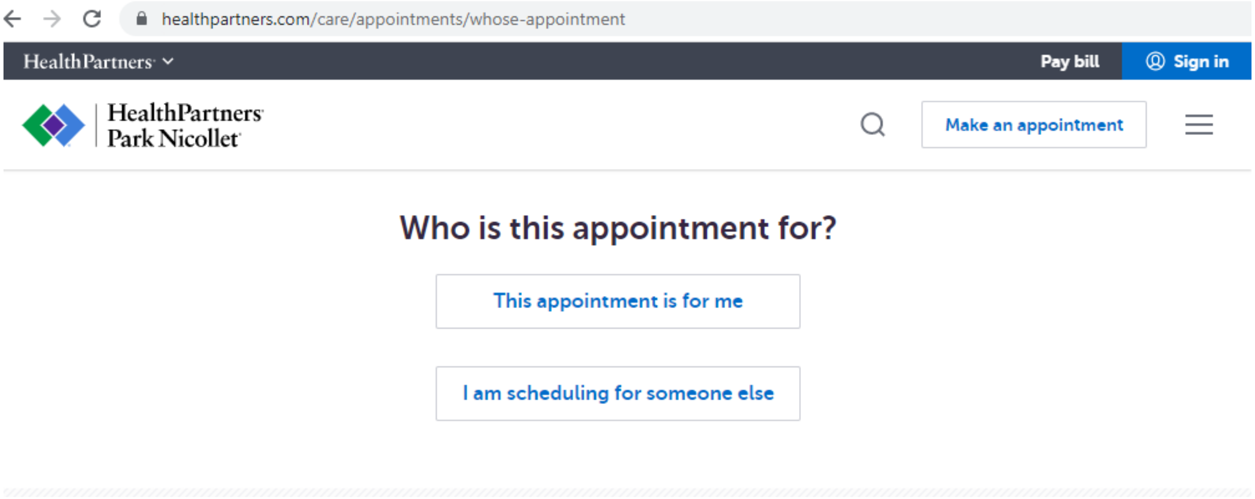
Talk with your care team

Have a question or need

Take your care on the go

Manage your care

153. Next, the user clicks the "This appointment is for me" button.

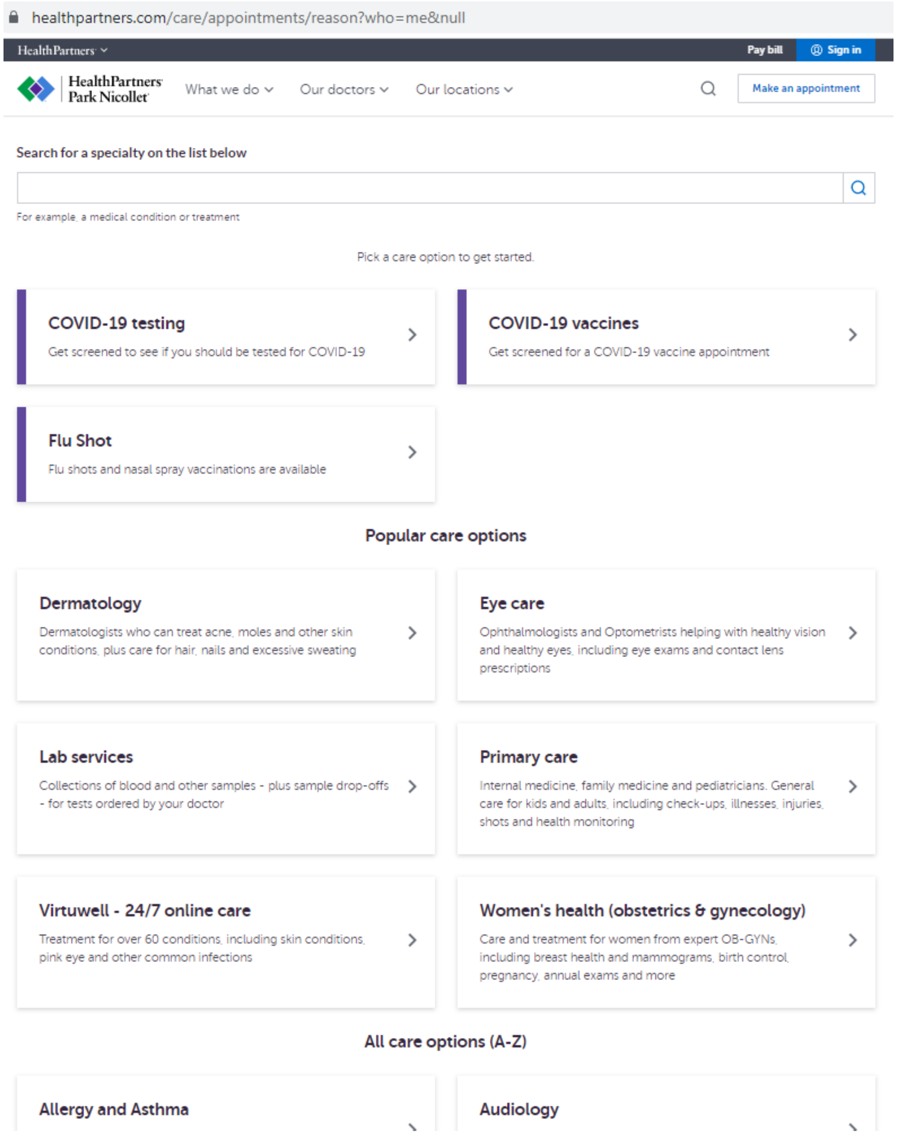


healthpartners.com/care/appointments/whose-appointment
HealthPartners
Pay bill
Sign in
HealthPartners Park Nicollet
Make an appointment

Who is this appointment for?

This appointment is for me
I am scheduling for someone else

154. Defendant then directs the user to narrow their appointment search results by either typing a medical condition or treatment into the search bar or choosing from a list of "popular care options" or "All care options (A-Z)."



healthpartners.com/care/appointments/reason?who=me&null

Search for a specialty on the list below

For example, a medical condition or treatment

Pick a care option to get started.

COVID-19 testing
Get screened to see if you should be tested for COVID-19

COVID-19 vaccines
Get screened for a COVID-19 vaccine appointment

Flu Shot
Flu shots and nasal spray vaccinations are available

Popular care options

Dermatology
Dermatologists who can treat acne, moles and other skin conditions, plus care for hair, nails and excessive sweating

Eye care
Ophthalmologists and Optometrists helping with healthy vision and healthy eyes, including eye exams and contact lens prescriptions

Lab services
Collections of blood and other samples - plus sample drop-offs - for tests ordered by your doctor

Primary care
Internal medicine, family medicine and pediatricians. General care for kids and adults, including check-ups, illnesses, injuries, shots and health monitoring

Virtuwell - 24/7 online care
Treatment for over 60 conditions, including skin conditions, pink eye and other common infections

Women's health (obstetrics & gynecology)
Care and treatment for women from expert OB-GYNs, including breast health and mammograms, birth control, pregnancy, annual exams and more

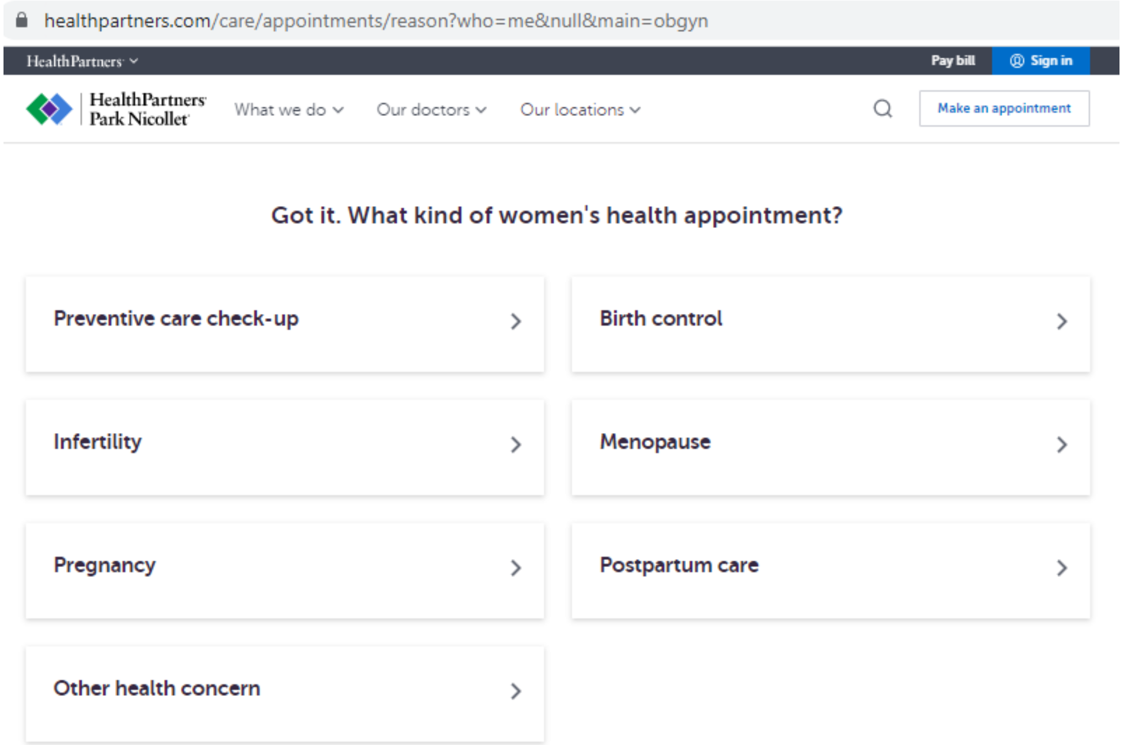
All care options (A-Z)

Allergy and Asthma

Audiology

155. The user clicks the "Women's health (obstetrics & gynecology)" button, and Defendant directs them to identify the "reason" for the appointment, or what type of

appointment the user believes they need, by selecting the course of treatment, symptom, or health condition for which they are seeking treatment.

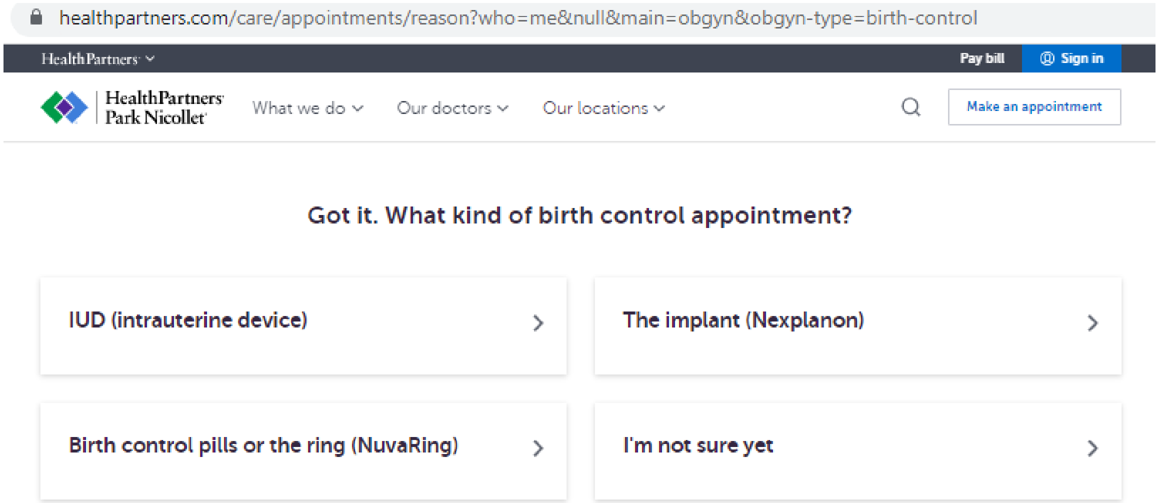


healthpartners.com/care/appointments/reason?who=me&null&main=obgyn

Got it. What kind of women's health appointment?

- Preventive care check-up
- Birth control
- Infertility
- Menopause
- Pregnancy
- Postpartum care
- Other health concern

156. Upon clicking the "birth control" button, Defendant asks the user to identify which type of treatment they are seeking.

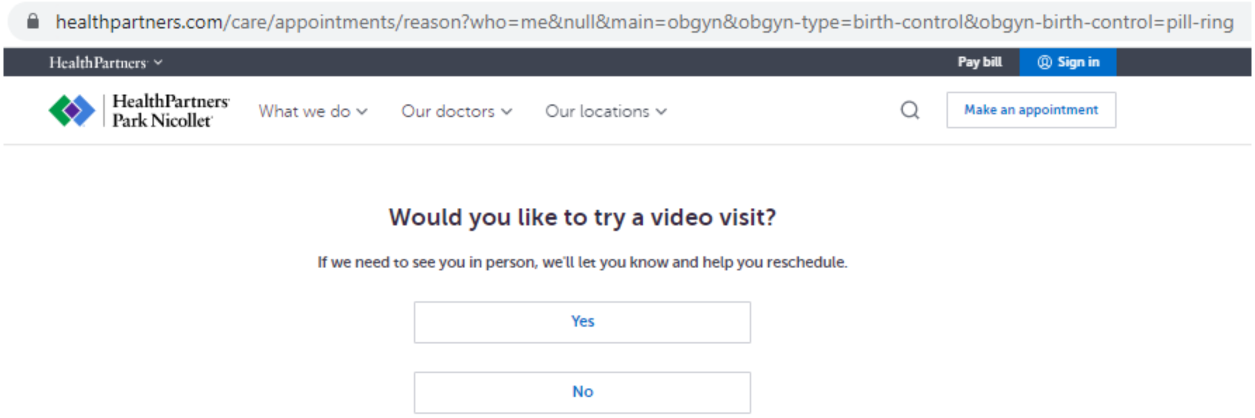


healthpartners.com/care/appointments/reason?who=me&null&main=obgyn&obgyn-type=birth-control

Got it. What kind of birth control appointment?

- IUD (intrauterine device)
- The implant (Nexplanon)
- Birth control pills or the ring (NuvaRing)
- I'm not sure yet

157. Upon clicking the “Birth control pills or the ring (NuvaRing)” button, Defendant asks whether the user would like to schedule a video visit or in-person appointment.

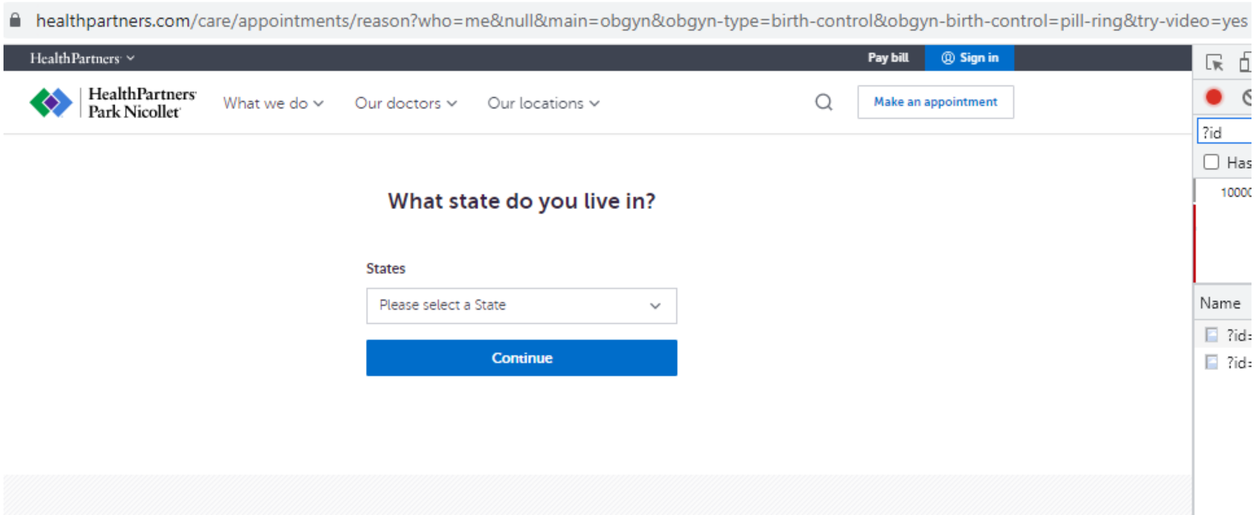


healthpartners.com/care/appointments/reason?who=me&null&main=obgyn&obgyn-type=birth-control&obgyn-birth-control=pill-ring

Would you like to try a video visit?

If we need to see you in person, we'll let you know and help you reschedule.

158. Upon clicking the “Yes” button, Defendant asks the user to identify their location, and the user selects Minnesota from the drop-down menu below.



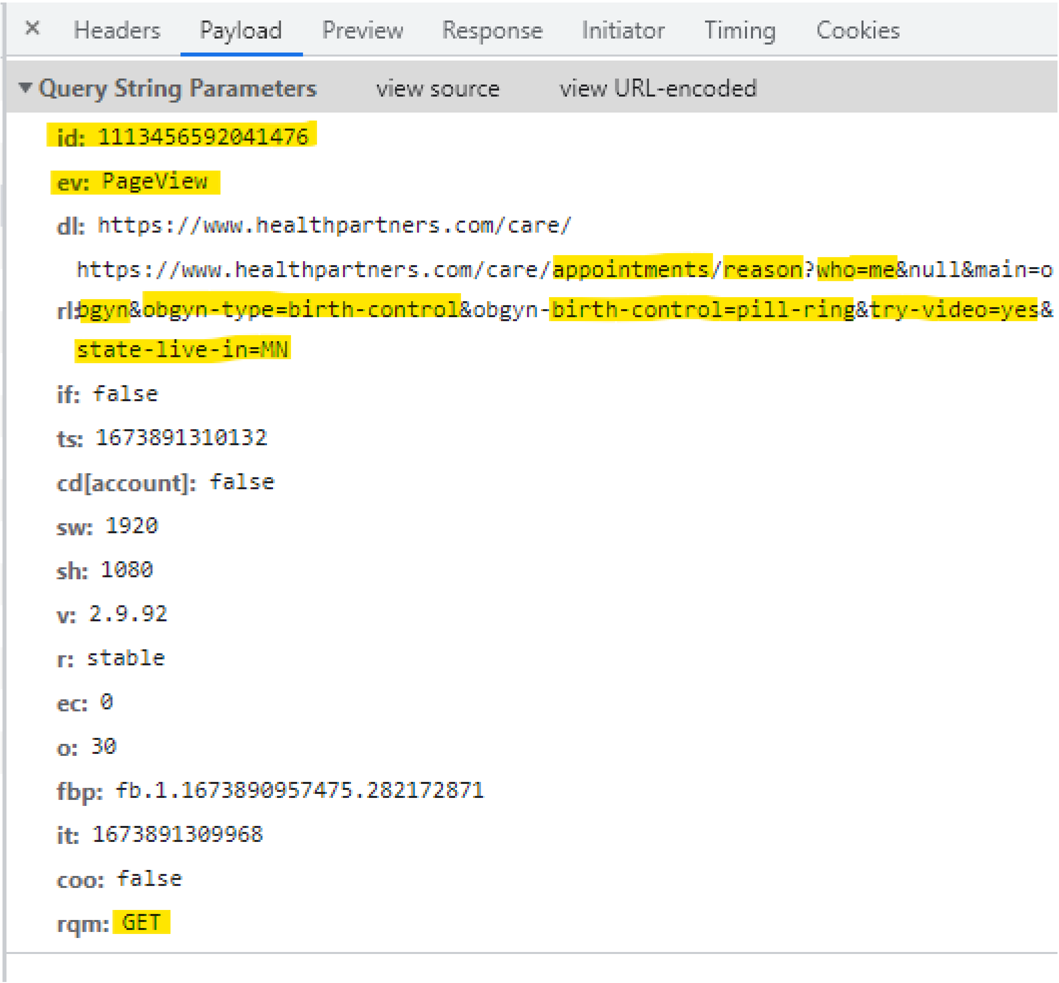
healthpartners.com/care/appointments/reason?who=me&null&main=obgyn&obgyn-type=birth-control&obgyn-birth-control=pill-ring&try-video=yes

What state do you live in?

States: Please select a State

159. Without alerting the user, Defendant’s Pixel sends each and every communication the user made to the Defendant via the Webpage to Facebook, and the

image below confirms that the communications Defendant sends to Facebook contain the user's Private Information.



```
id: 1113456592041476
ev: PageView
dl: https://www.healthpartners.com/care/
  https://www.healthpartners.com/care/appointments/reason?who=me&null&main=o
rl:bgyn&obgyn-type=birth-control&obgyn-birth-control=pill-ring&try-video=yes&
  state-live-in=MN
if: false
ts: 1673891310132
cd[account]: false
sw: 1920
sh: 1080
v: 2.9.92
r: stable
ec: 0
o: 30
fbp: fb.1.1673890957475.282172871
it: 1673891309968
coo: false
rqm: GET
```

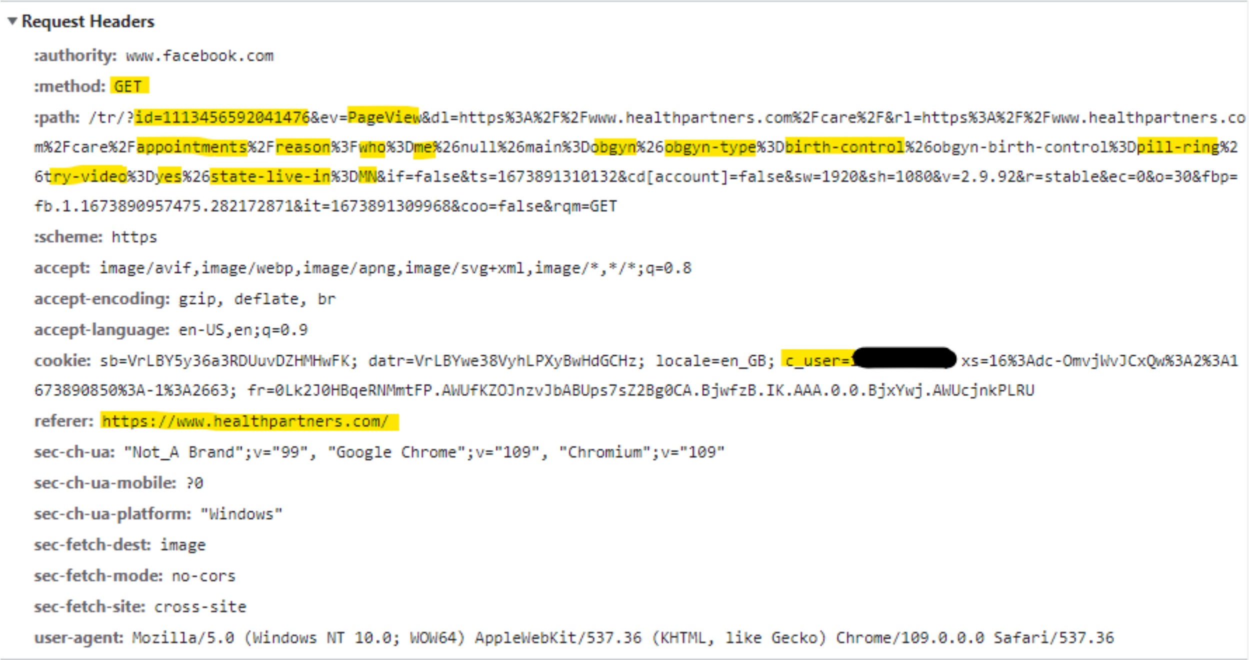
160. The first line of highlighted text, "id: 1113456592041476," refers to the Defendant's Pixel ID for this particular Webpage and confirms that the Defendant has downloaded the Pixel into its Source Code on this particular Webpage.

161. The second line of text, "ev: PageView," identifies and categorizes which actions the user took on the Webpage ("ev:" is an abbreviation for event, and "PageView" is the type of event). Thus, this identifies the user as having viewed the particular Webpage.

162. The remaining lines of text identify: (1) the user as a patient seeking medical care from Defendant via www.healthpartners.com; (2) who is in the process of booking an "appointment"; (3) the appointment is for herself as opposed to someone else (appearing as "who=me" in the text above); (4) the appointment is with an "obgyn" (aka the "reason" for the appointment); (5) the medical treatment and sought medication is "birth control"; (6) the user has identified which type of birth control they desire ("pill-ring"); (7) the user's location ("state-live-in=MN" with "MN"(Minnesota); and (8) the fact that the user's appointment will be via video instead of in-person ("try-video=yest").

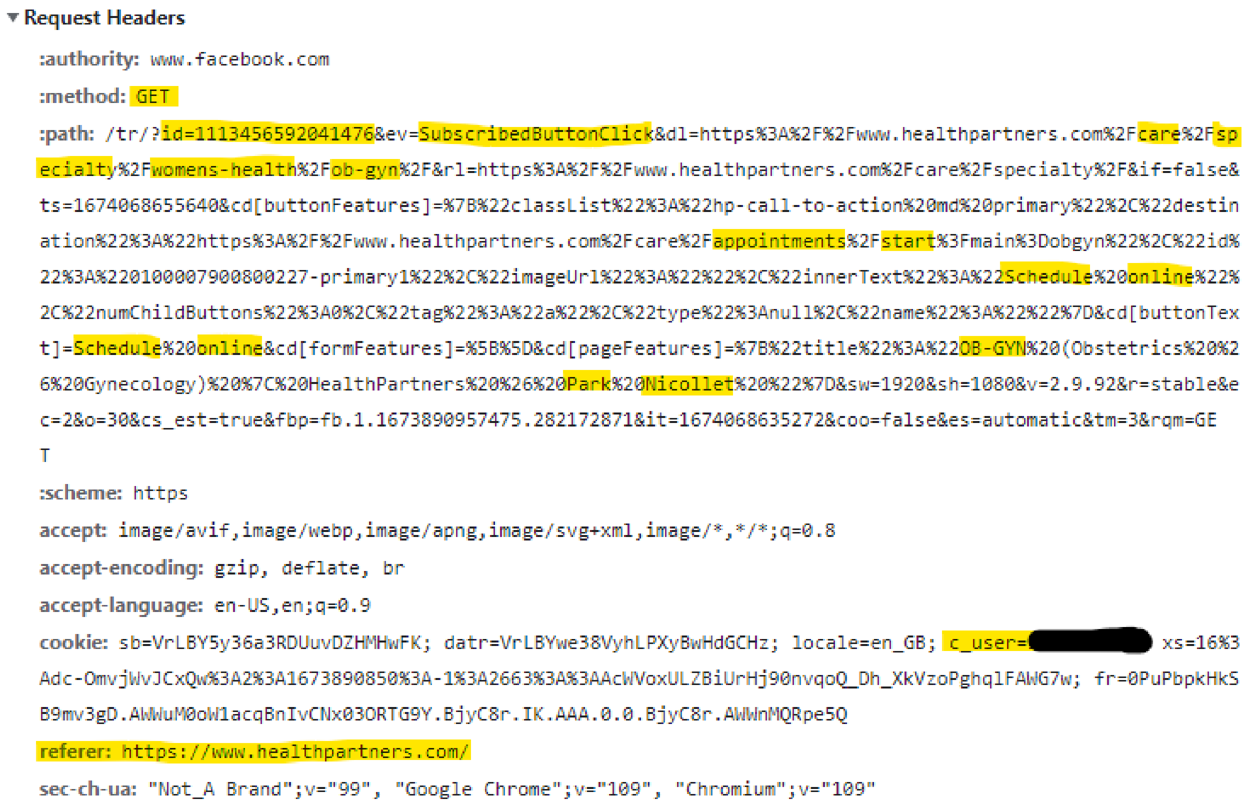
163. Finally, the last line of highlighted text ("GET"), demonstrates the user's communications, and Private Information contained therein, are sent to Facebook alongside their Facebook ID (c_user ID cookie). This is further evidenced by the image below, which was collected during the same browsing session as the previous image.[36]

[36] The user's Facebook ID is represented as the c_user ID highlight in the image above, and Plaintiffs have redacted the corresponding string of numbers to preserve the user's anonymity.



```
▼ Request Headers
    :authority: www.facebook.com
    :method: GET
    :path: /tr/?id=1113456592041476&ev=PageView&dl=https%3A%2F%2Fwww.healthpartners.com%2Fcare%2F&rl=https%3A%2F%2Fwww.healthpartners.co
    m%2Fcare%2Fappointments%2Freason%3Fwho%3Dme%26null%26main%3Dobgyn%26obgyn-type%3Dbirth-control%26obgyn-birth-control%3Dpill-ring%2
    6try-video%3Dyes%26state-live-in%3DMN&if=false&ts=1673891310132&cd[account]=false&sw=1920&sh=1080&v=2.9.92&r=stable&ec=0&o=30&fbp=
    fb.1.1673890957475.282172871&it=1673891309968&coo=false&rqm=GET
    :scheme: https
    accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
    accept-encoding: gzip, deflate, br
    accept-language: en-US,en;q=0.9
    cookie: sb=VrLBY5y36a3RDUuvDZHMHwFK; datr=VrLBYwe38VyhLPXyBwHdGCHz; locale=en_GB; c_user=[redacted] xs=16%3Adc-OmvjWvJCxQw%3A2%3A1
    673890850%3A-1%3A2663; fr=0Lk2J0HBqeRNMmtFP.AWUfKZOJnzvJbABUps7sZ2Bg0CA.BjwfzB.IK.AAA.0.0.BjxYwj.AWUcjnkPLRU
    referer: https://www.healthpartners.com/
    sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
    sec-ch-ua-mobile: ?0
    sec-ch-ua-platform: "Windows"
    sec-fetch-dest: image
    sec-fetch-mode: no-cors
    sec-fetch-site: cross-site
    user-agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
```

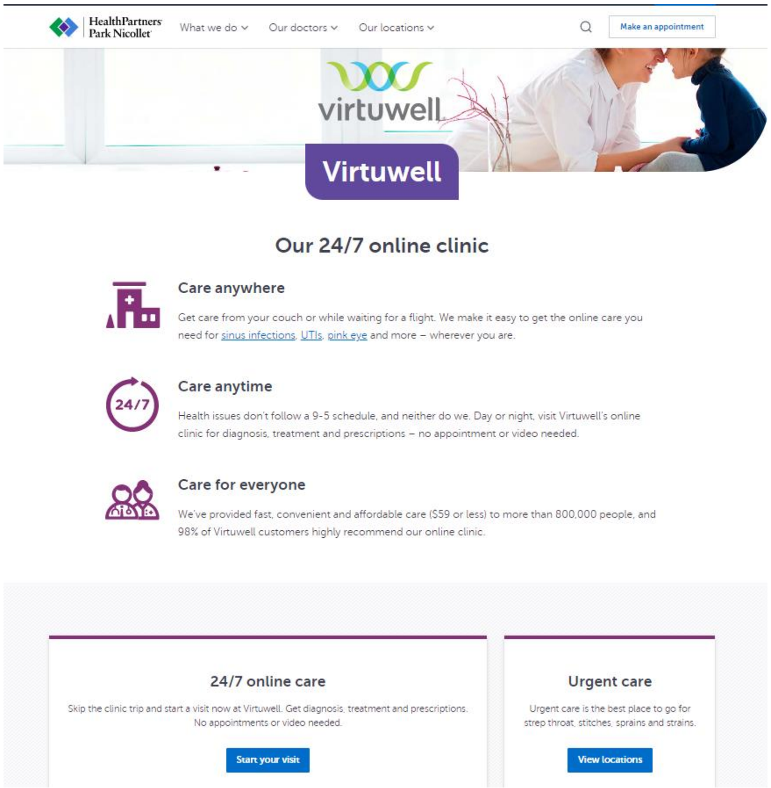
164. In addition to tracking its patients' "PageViews," Defendant's Pixel is also tracking and transmitting information about which buttons a user clicks or selects during their browsing session. In the example below, the user's Webpage activity is categorized and communicated to Facebook as a "SubscribedButtonClick," indicating which buttons the user selected on the Webpage.



```
▼ Request Headers
   :authority: www.facebook.com
   :method: GET
   :path: /tr/?id=1113456592041476&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.healthpartners.com%2Fcare%2Fsp
   ecialty%2Fwomens-health%2Fob-gyn%2F&rl=https%3A%2F%2Fwww.healthpartners.com%2Fcare%2Fspecialty%2F&if=false&
   ts=1674068655640&cd[buttonFeatures]=%7B%22classList%22%3A%22hp-call-to-action%20md%20primary%22%2C%22destin
   ation%22%3A%22https%3A%2F%2Fwww.healthpartners.com%2Fcare%2Fappointments%2Fstart%3Fmain%3Dobgyn%22%2C%22id%
   22%3A%22010000790080O227-primary1%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Schedule%20online%22%
   2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonTex
   t]=Schedule%20online&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22OB-GYN%20(Obstetrics%20%2
   6%20Gynecology)%20%7C%20HealthPartners%20%26%20Park%20Nicollet%20%22%7D&sw=1920&sh=1080&v=2.9.92&r=stable&e
   c=2&o=30&cs_est=true&fbp=fb.1.1673890957475.282172871&it=1674068635272&coo=false&es=automatic&tm=3&rqm=GE
   T
   :scheme: https
   accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
   accept-encoding: gzip, deflate, br
   accept-language: en-US,en;q=0.9
   cookie: sb=VrLBY5y36a3RDUuvDZHMHwFK; datr=VrLBYwe38VyhLPXyBwHdGCHz; locale=en_GB; c_user=[redacted] xs=16%3
   Adc-OmvjWvJCxQw%3A2%3A1673890850%3A-1%3A2663%3A%3AAcWVoxULZBiUrHj90nvqoQ_Dh_XkVzoPghqlFAWG7w; fr=0PuPbpkHkS
   B9mv3gD.AWWuM0oW1acqBnIvCNx03ORTG9Y.BjyC8r.IK.AAA.0.0.BjyC8r.AWWnMQRpe5Q
   referer: https://www.healthpartners.com/
   sec-ch-ua: "Not_A Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
```

ii. Defendant's Pixel Disseminates Patient Information via Virtuwell.com and other Websites

165. Defendant encourages its patients to use "Virtuwell," which it describes as a "24/7 online clinic." Upon clicking the "Start your visit" button in the image below, Defendant directs the user to virtuwell.com where the user must click the "Get started" button to continue.



Virtuwell

Our 24/7 online clinic

Care anywhere

Get care from your couch or while waiting for a flight. We make it easy to get the online care you need for sinus infections, UTIs, pink eye and more – wherever you are.

Care anytime

Health issues don't follow a 9-5 schedule, and neither do we. Day or night, visit Virtuwell's online clinic for diagnosis, treatment and prescriptions – no appointment or video needed.

Care for everyone

We've provided fast, convenient and affordable care ($59 or less) to more than 800,000 people, and 98% of Virtuwell customers highly recommend our online clinic.

24/7 online care

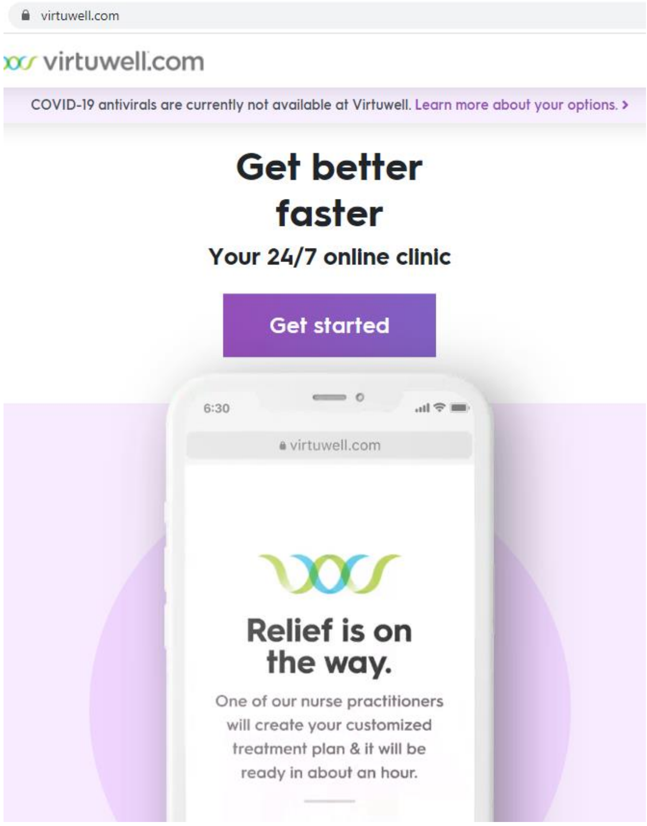
Skip the clinic trip and start a visit now at Virtuwell. Get diagnosis, treatment and prescriptions. No appointments or video needed.

Start your visit

Urgent care

Urgent care is the best place to go for strep throat, stitches, sprains and strains.

View locations



COVID-19 antivirals are currently not available at Virtuwell. Learn more about your options. >

Get better faster

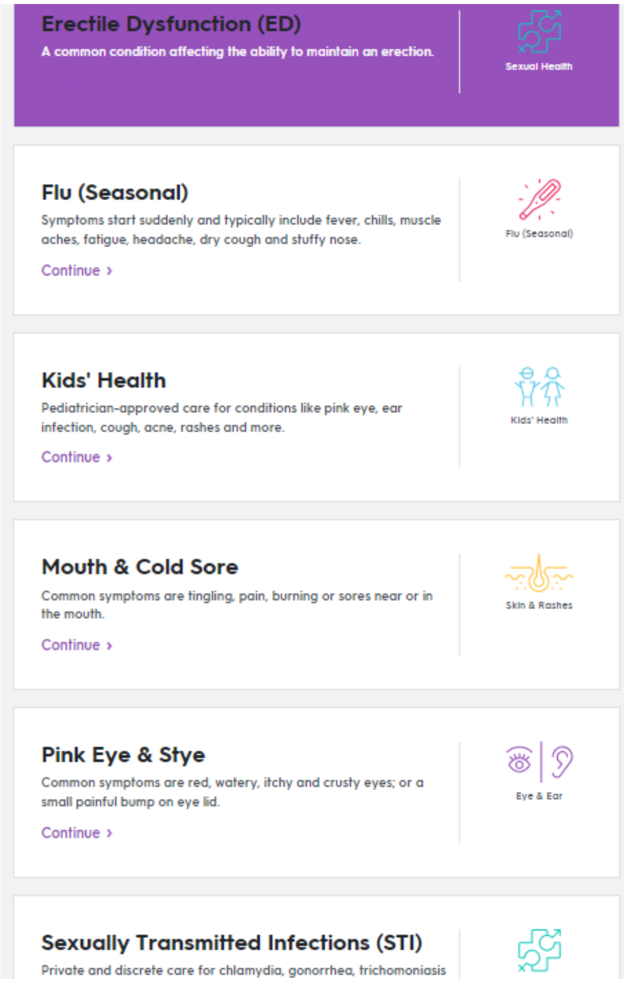
Your 24/7 online clinic

Get started

Relief is on the way.

One of our nurse practitioners will create your customized treatment plan & it will be ready in about an hour.

166. Next, Defendant asks the user to identify what type of treatment they are seeking by selecting the health condition or symptom they are experiencing. The user selects “Mouth & Cold Sore” and clicks the “Continue” button.



Erectile Dysfunction (ED)
A common condition affecting the ability to maintain an erection.

Flu (Seasonal)
Symptoms start suddenly and typically include fever, chills, muscle aches, fatigue, headache, dry cough and stuffy nose.
Continue ›

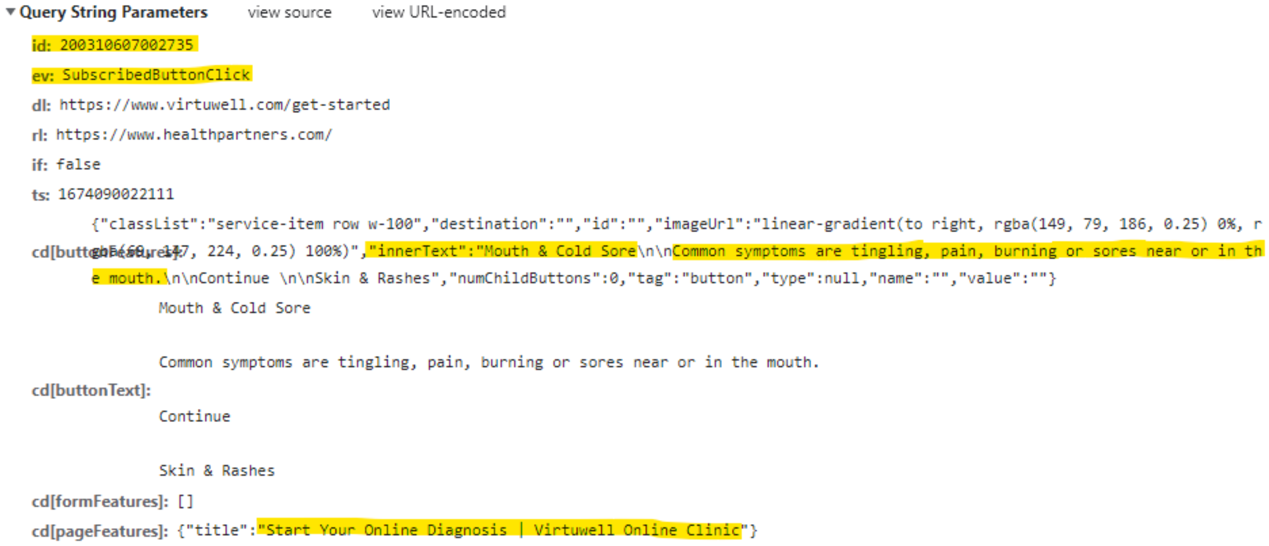
Kids' Health
Pediatrician-approved care for conditions like pink eye, ear infection, cough, acne, rashes and more.
Continue ›

Mouth & Cold Sore
Common symptoms are tingling, pain, burning or sores near or in the mouth.
Continue ›

Pink Eye & Stye
Common symptoms are red, watery, itchy and crusty eyes; or a small painful bump on eye lid.
Continue ›

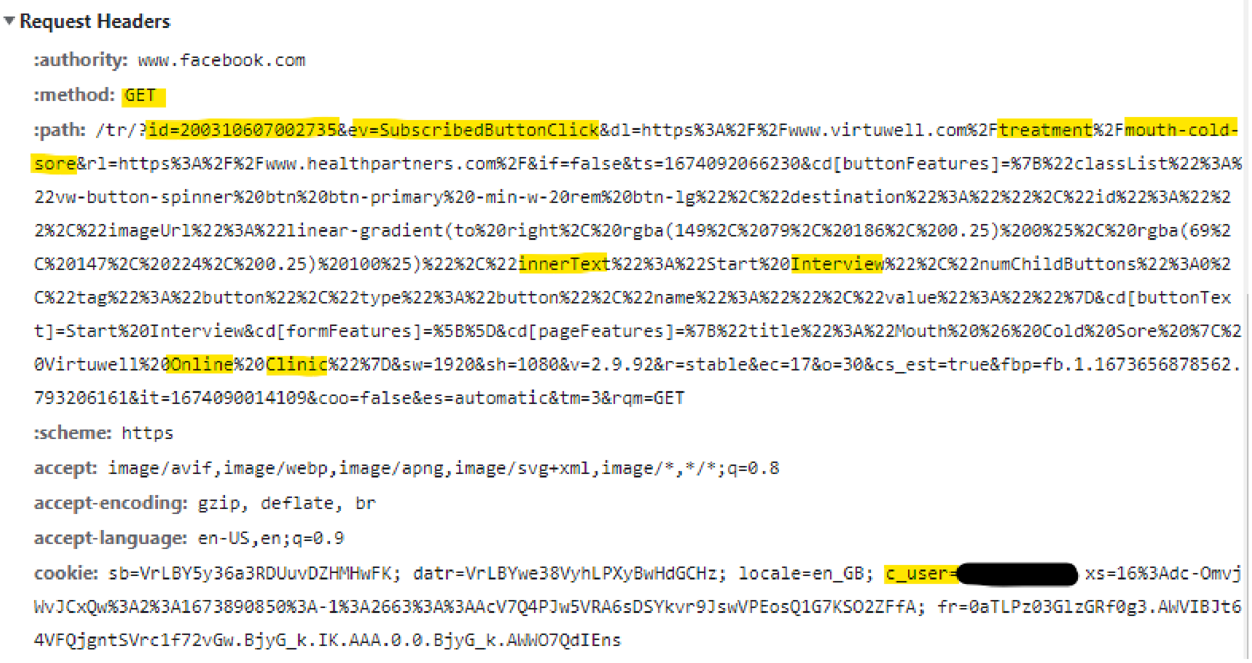
Sexually Transmitted Infections (STI)
Private and discrete care for chlamydia, gonorrhea, trichomoniasis

167. Upon doing so, Defendant’s Pixel records the user’s activity as a “SubscribedButtonClick” event and sends that information to Facebook. The image below demonstrates that Defendant’s Pixel is located on this particular Webpage (recorded as id: 200310607002735 for this particular Webpage and highlighted in the image below).



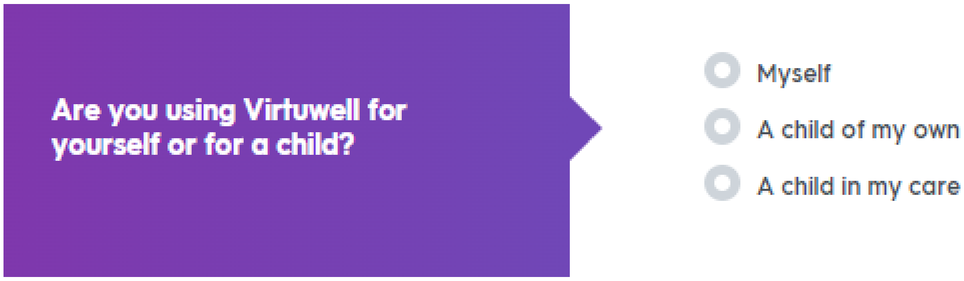
```
▼ Query String Parameters     view source     view URL-encoded
   id: 200310607002735
   ev: SubscribedButtonClick
   dl: https://www.virtuwell.com/get-started
   rl: https://www.healthpartners.com/
   if: false
   ts: 1674090022111
          {"classList":"service-item row w-100","destination":"","id":"","imageUrl":"linear-gradient(to right, rgba(149, 79, 186, 0.25) 0%, r
   cd[buttonFeatures]: gba(69, 147, 224, 0.25) 100%)","innerText":"Mouth & Cold Sore\n\nCommon symptoms are tingling, pain, burning or sores near or in th
          e mouth.\n\nContinue \n\nSkin & Rashes","numChildButtons":0,"tag":"button","type":null,"name":"","value":""}
                   Mouth & Cold Sore

                   Common symptoms are tingling, pain, burning or sores near or in the mouth.
   cd[buttonText]:
                   Continue

                   Skin & Rashes
   cd[formFeatures]: []
   cd[pageFeatures]: {"title":"Start Your Online Diagnosis | Virtuwell Online Clinic"}
```

168. Next, the user clicks "Start Interview." Upon doing so, Defendant's Pixel records and transmits the user's activity to Facebook, categorizing it as a "SubscribedButtonClick" event, "AddToCart" event, and "PageView." As with previous examples, Defendant's Pixel sends this information alongside the user's unique and persistent Facebook ID.



```
▼ Request Headers
   :authority: www.facebook.com
   :method: GET
   :path: /tr/?id=200310607002735&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.virtuwell.com%2Ftreatment%2Fmouth-cold-
   sore&rl=https%3A%2F%2Fwww.healthpartners.com%2F&if=false&ts=1674092066230&cd[buttonFeatures]=%7B%22classList%22%3A%
   22vw-button-spinner%20btn%20btn-primary%20-min-w-20rem%20btn-lg%22%2C%22destination%22%3A%22%22%2C%22id%22%3A%22%2
   2%2C%22imageUrl%22%3A%22linear-gradient(to%20right%2C%20rgba(149%2C%2079%2C%20186%2C%200.25)%200%25%2C%20rgba(69%2
   C%20147%2C%20224%2C%200.25)%20100%25)%22%2C%22innerText%22%3A%22Start%20Interview%22%2C%22numChildButtons%22%3A0%2
   C%22tag%22%3A%22button%22%2C%22type%22%3A%22button%22%2C%22name%22%3A%22%22%2C%22value%22%3A%22%22%7D&cd[buttonTex
   t]=Start%20Interview&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Mouth%20%26%20Cold%20Sore%20%7C%2
   0Virtuwell%20Online%20Clinic%22%7D&sw=1920&sh=1080&v=2.9.92&r=stable&ec=17&o=30&cs_est=true&fbp=fb.1.1673656878562.
   793206161&it=1674090014109&coo=false&es=automatic&tm=3&rqm=GET
   :scheme: https
   accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
   accept-encoding: gzip, deflate, br
   accept-language: en-US,en;q=0.9
   cookie: sb=VrLBY5y36a3RDUuvDZHMHwFK; datr=VrLBYwe38VyhLPXyBwHdGCHz; locale=en_GB; c_user=[redacted] xs=16%3Adc-Omvj
   WvJCxQw%3A2%3A1673890850%3A-1%3A2663%3A%3AAcV7Q4PJw5VRA6sDSYkvr9JswVPEosQ1G7KSO2ZFfA; fr=0aTLPz03GlzGRf0g3.AWVIBJt6
   4VFQjgntSVrc1f72vGw.BjyG_k.IK.AAA.0.0.BjyG_k.AWWO7QdIEns
```

169. Then, Defendant asks the user to specify who the medical appointment is for and once again surreptitiously transmits that information when the user selects “Myself and clicks “Continue.”



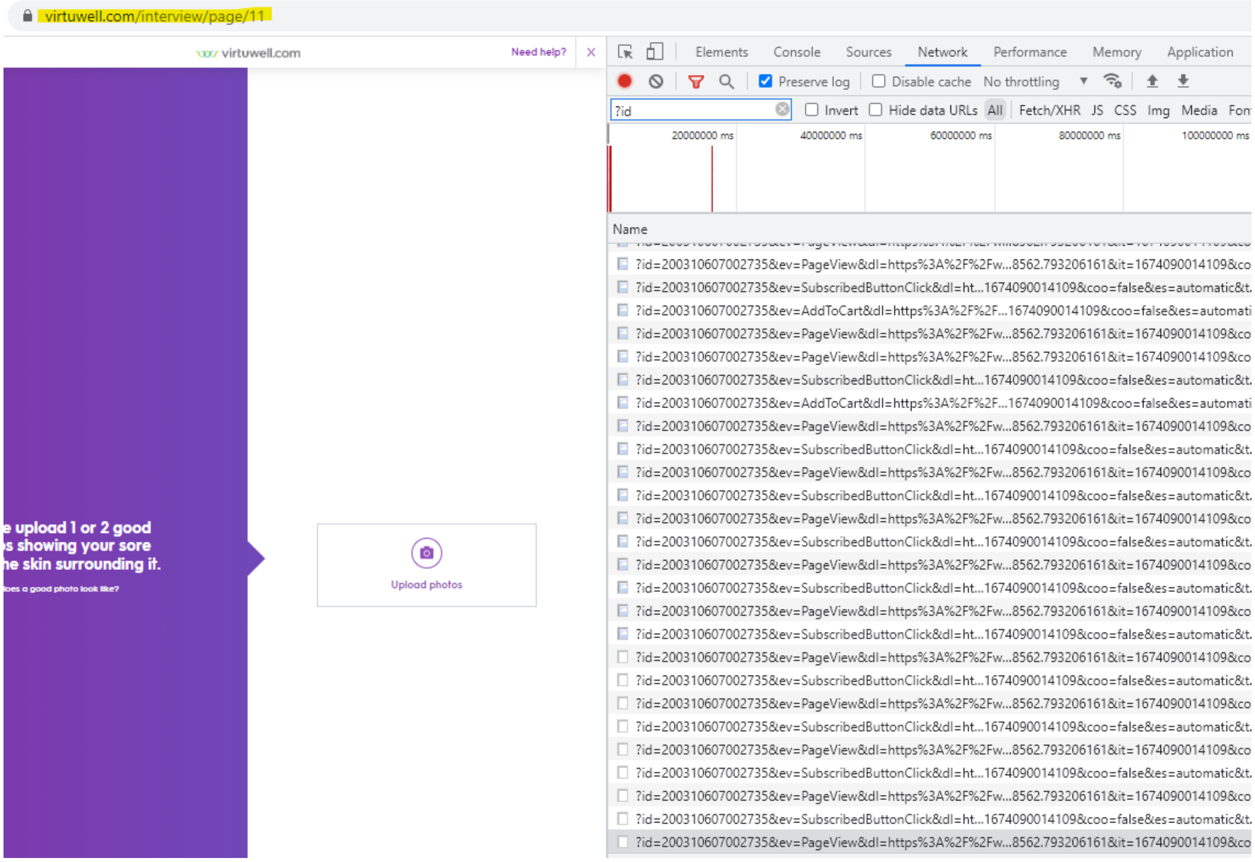
Are you using Virtuwell for yourself or for a child?

○ Myself

○ A child of my own

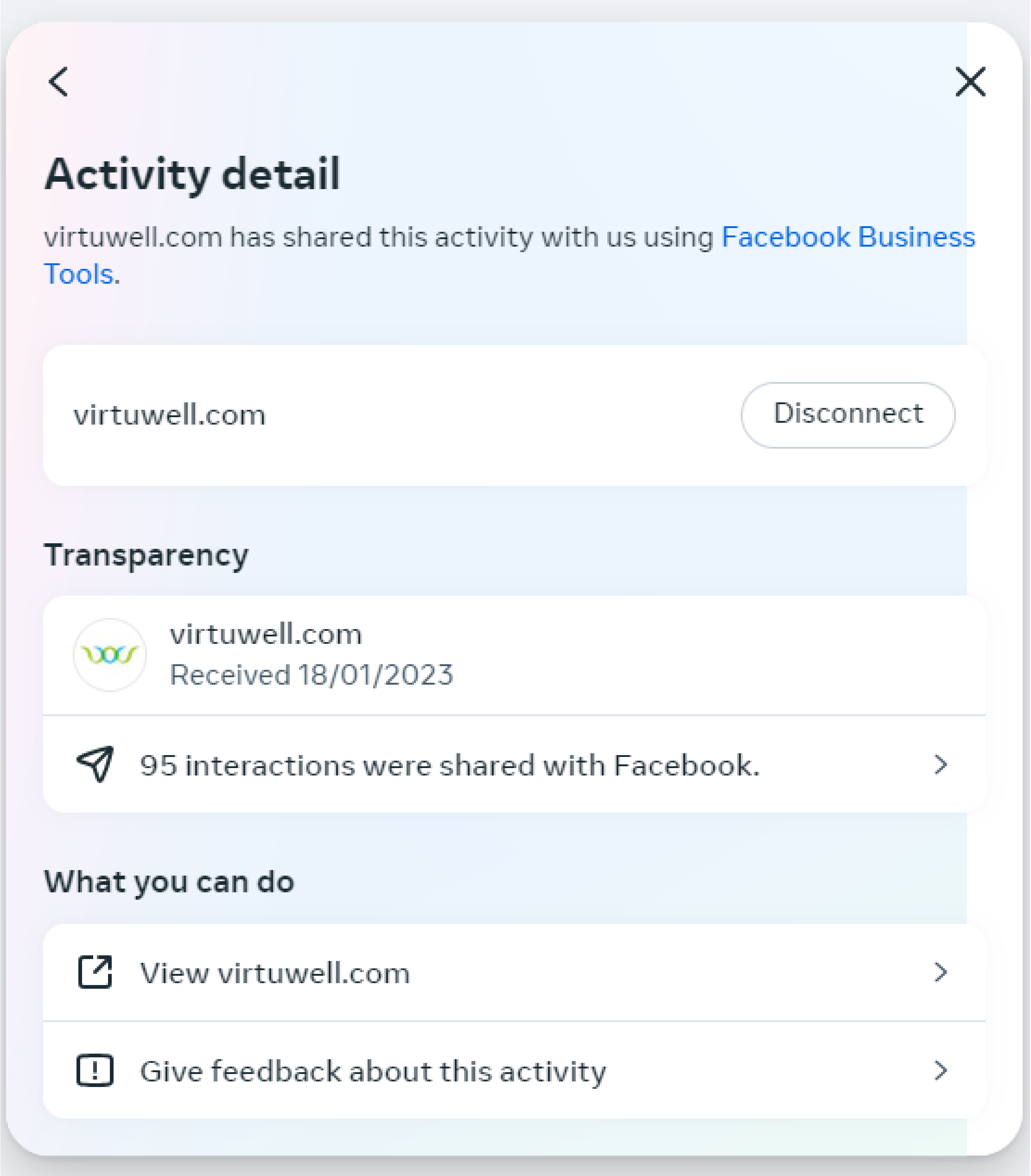
○ A child in my care

As the user continues through the interview process, they are asked to communicate additional PHI and PII on each new Webpage, the responses containing their PHI and PII has been sent to Facebook approximately 25 times. The image below is a screenshot taken from the network track report associated with virtuwell.com/interview/page/11, and every entry in the right column represents one instance in which the user’s communications with Defendant were transmitted to Facebook as a result of Defendant’s tracking and dissemination practices.



```
?id=20031060700273 5&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=AddToCart&dl=https%3A%2F%2F...1674090014109&coo=false&es=automati
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=AddToCart&dl=https%3A%2F%2F...1674090014109&coo=false&es=automati
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
?id=200310607002735&ev=SubscribedButtonClick&dl=ht...1674090014109&coo=false&es=automatic&t.
?id=200310607002735&ev=PageView&dl=https%3A%2F%2Fw...8562.793206161&it=1674090014109&co
```

170. Facebook undoubtedly receives this information, and this can be confirmed by the image below, which is a screenshot taken from the user's "Off Facebook Activity Report."



Activity detail

virtuwell.com has shared this activity with us using Facebook Business Tools.

virtuwell.com

Transparency

virtuwell.com
Received 18/01/2023

95 interactions were shared with Facebook.

What you can do

171. As shown above, at least 95 of the user's communications to Defendant were sent to and received by Facebook as of January 18, 2023, as a result of using virtuwell.com. Facebook expressly states, "virtuwell.com has shared this activity with us using Facebook Business tools."

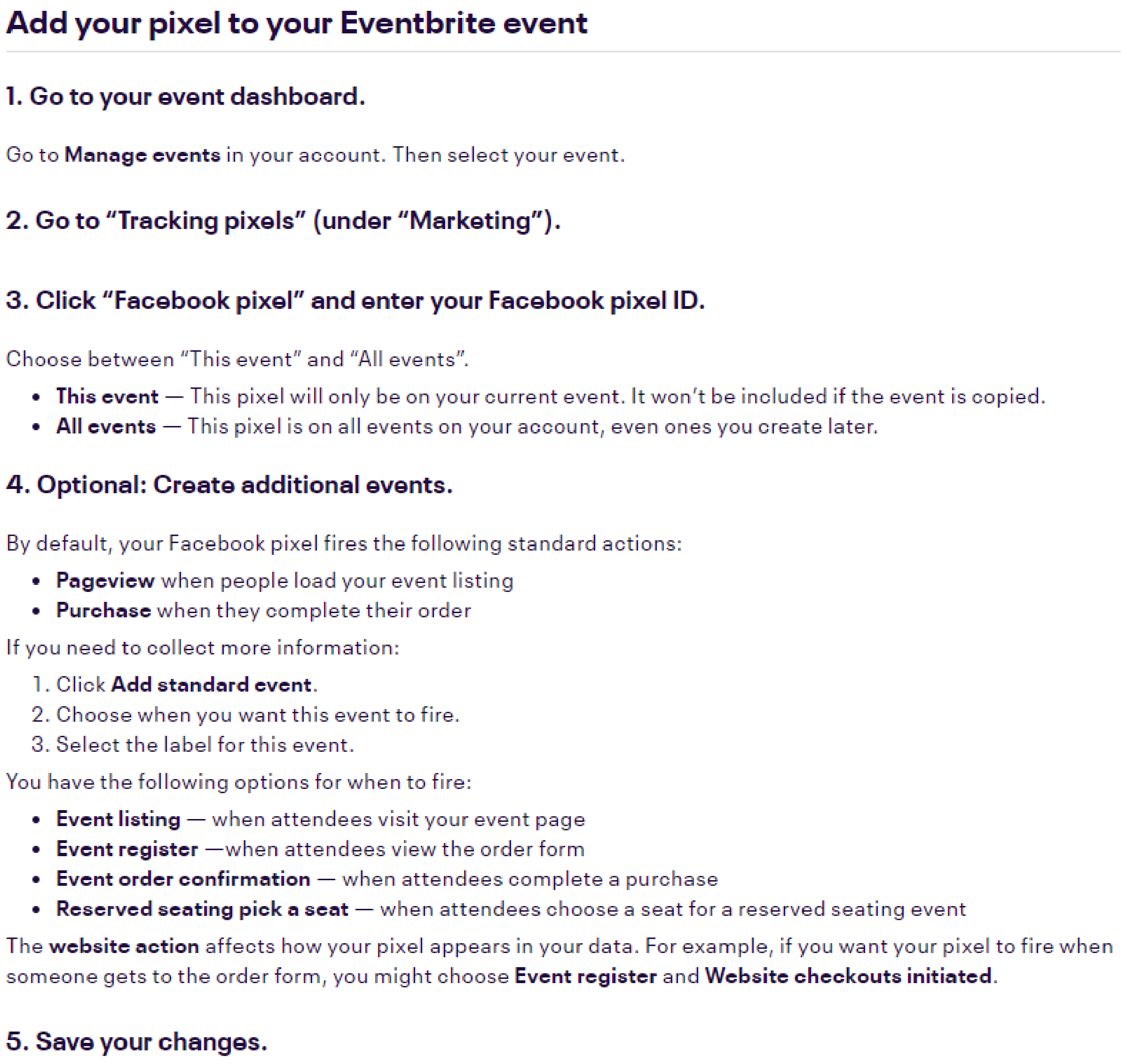
172. Defendant’s practice of transmitting its patients’ data extends beyond its own Website. For example, Defendant offers and encourages its patients to sign up for healthcare classes, events, and support groups including breastfeeding courses, a “Community Foot Care Clinic,” “Better Breathers” courses, and “Stomp out diabetes” online courses. If a patient attempts to book an online breastfeeding course, Defendant’s Webpage redirects the patient to a third-party website to complete their booking (https://www.eventbrite.com/e/breastfeeding-online-stillwater-registration-444739205937).

173. From there, the patient can select a desired date, submit additional information, and purchase the event ticket.

174. As with the other examples, the patient’s information is communicated to Facebook via Defendant’s Pixel, and Defendant has purposefully designed its events to track patient’s activity and communications.

175. The tracking that occurs is not the result of a pre-programmed function, but rather a purposeful decision made by Defendant. As the instructions below explain, Eventbrite allows the event host (Defendant) to configure and program a particular event’s webpage.[37] In conjunction with this, the event host can upload their tracking pixel.

[37] *Add a Facebook Pixel to Your Event*, Eventbrite Help Center, https://www.eventbrite.com/support/articles/en_US/Multi_Group_How_To/how-to-create-a-tracking-pixel-with-facebook?lg=en_US (last visited July 11, 2023).



Add your pixel to your Eventbrite event

1. Go to your event dashboard.

Go to **Manage events** in your account. Then select your event.

2. Go to "Tracking pixels" (under "Marketing").

3. Click "Facebook pixel" and enter your Facebook pixel ID.

Choose between "This event" and "All events".

- **This event** — This pixel will only be on your current event. It won't be included if the event is copied.
- **All events** — This pixel is on all events on your account, even ones you create later.

4. Optional: Create additional events.

By default, your Facebook pixel fires the following standard actions:

- **Pageview** when people load your event listing
- **Purchase** when they complete their order

If you need to collect more information:

1. Click **Add standard event**.
2. Choose when you want this event to fire.
3. Select the label for this event.

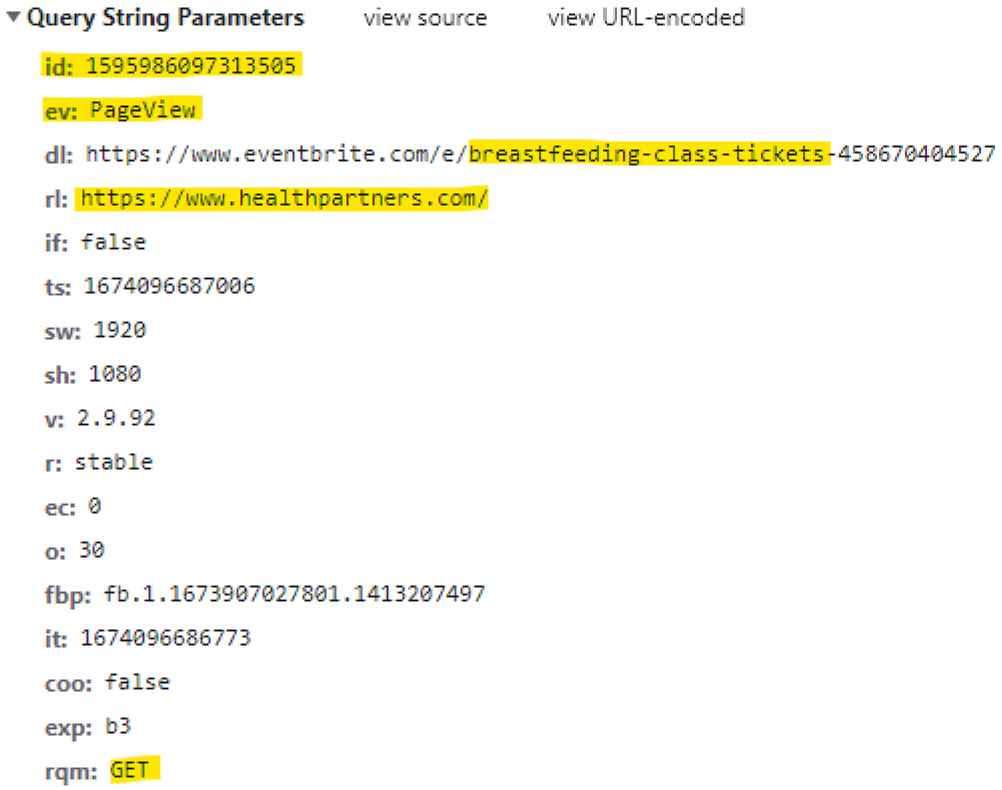
You have the following options for when to fire:

- **Event listing** — when attendees visit your event page
- **Event register** —when attendees view the order form
- **Event order confirmation** — when attendees complete a purchase
- **Reserved seating pick a seat** — when attendees choose a seat for a reserved seating event

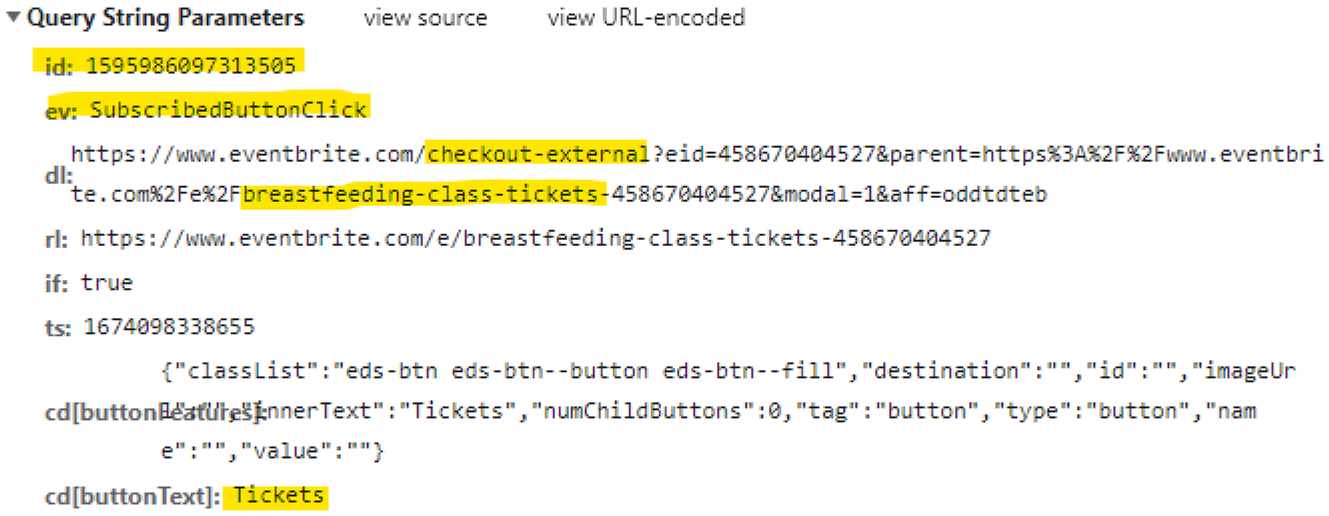
The **website action** affects how your pixel appears in your data. For example, if you want your pixel to fire when someone gets to the order form, you might choose **Event register** and **Website checkouts initiated**.

5. Save your changes.

176. Correspondingly, on information and belief, the images below demonstrate that Defendant has indeed implemented its Pixel to track and transmit information to Facebook whenever patients book healthcare related courses.



```
▼ Query String Parameters     view source     view URL-encoded
    id: 1595986097313505
    ev: PageView
    dl: https://www.eventbrite.com/e/breastfeeding-class-tickets-458670404527
    rl: https://www.healthpartners.com/
    if: false
    ts: 1674096687006
    sw: 1920
    sh: 1080
    v: 2.9.92
    r: stable
    ec: 0
    o: 30
    fbp: fb.1.1673907027801.1413207497
    it: 1674096686773
    coo: false
    exp: b3
    rqm: GET
```



```
▼ Query String Parameters     view source     view URL-encoded
    id: 1595986097313505
    ev: SubscribedButtonClick
    dl: https://www.eventbrite.com/checkout-external?eid=458670404527&parent=https%3A%2F%2Fwww.eventbri
        te.com%2Fe%2Fbreastfeeding-class-tickets-458670404527&modal=1&aff=oddtdteb
    rl: https://www.eventbrite.com/e/breastfeeding-class-tickets-458670404527
    if: true
    ts: 1674098338655
    cd[buttonFeatures]: {"classList":"eds-btn eds-btn--button eds-btn--fill","destination":"","id":"","imageUr
        l":"","innerText":"Tickets","numChildButtons":0,"tag":"button","type":"button","nam
        e":"","value":""}
    cd[buttonText]: Tickets
```

iii. Facebook Exploited and Used Plaintiffs' and Class Members' Private Information.

177. Unsurprisingly, Facebook does not offer its Pixel to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"[38] and Meta has built its more-than $800 billion market capitalization on mining and using that "digital" oil. Thus, the large volumes of personal and sensitive health-related data Defendant provided to Facebook are actively viewed, examined, analyzed, curated, and put to use by the company. Facebook acquires the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Facebook offers the Pixel free of charge[39] and the price that Defendant pays for the Pixel is the data that it allows Facebook to collect.

178. Facebook sells advertising space by emphasizing its ability to target users.[40] Facebook is especially effective at targeting users because it surveils user activity both on and off its site (with the help of companies like Defendant).[41] This allows Facebook to make inferences about users beyond what they explicitly disclose, including their

[38] Joris Toonders, *Data is the New Oil of the Digital Economy*, WIRED (July 2014), https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last visited July 11, 2023).

[39] *Facebook Pixel: What It Is and Why You Need It*, SeoDigital, https://seodigitalgroup.com/facebook-pixel/ (last visited July 11, 2023).

[40] *Why Advertise on Facebook, Instagram and other Meta Technologies*, Meta Business Help Center, https://www.facebook.com/business/help/205029060038706 (last visited July 11, 2023).

[41] *About Meta Pixel*, Meta Business Help Center, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited July 11, 2023).

"interests," "behavior," and "connections."[42] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[43]

179. Advertisers can also build "Custom Audiences,"[44] which helps them reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[45] With Custom Audiences, advertisers can target existing customers directly. They can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[46] Unlike Core Audiences, Custom Audiences and Lookalike Audiences are only available if the advertiser has sent its underlying data to Facebook. This data can be supplied to

[42] *Audience Ad Targeting*, Meta Ads, https://www.facebook.com/business/ads/ad-targeting (last visited July 11, 2023).

[43] *Core Audiences*, Meta Ads, https://www.facebook.com/business/news/Core-Audiences (last visited July 11, 2023).

[44] *About Custom Audiences*, Meta Business Help Center, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited July 11, 2023).

[45] *Audience Ad Targeting*, Meta Ads, https://www.facebook.com/business/ads/ad-targeting (last visited July 11, 2023).

[46] *About Lookalike Audiences*, Meta Business Help Center, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited July 11, 2023).

Facebook by manually uploading contact information for customers or by utilizing Facebook's "Business Tools" like the Pixel and CAPI.[47]

180. Facebook does not merely collect information gathered by the Pixel and store it for safekeeping on its servers without ever viewing or accessing the information. Instead, in accordance with the purpose of the Pixel to allow Facebook to create Core, Custom, and Lookalike Audiences for advertising and marketing purposes, Facebook viewed, processed, and analyzed Plaintiffs' and Class Members' confidential Private Information. Upon information and belief, such viewing, processing, and analyzing was performed by computers and/or algorithms programmed and designed by Facebook employees at the direction and behest of Facebook.

181. Facebook receives over 4 petabytes[48] of information every day and must rely on analytical tools designed to view, categorize, and extrapolate the data to augment human

[47] *Create a Customer List Custom Audience,* Meta Business Help Center, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited July 11, 2023); *Create a Website Custom Audience,* Meta Business Help Center, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited July 11, 2023).

[48] A petabyte is equal to one million gigabytes (1,000,000 GB).

effort.[49] This process is known as "data ingestion" and allows "businesses to manage and make sense of large amounts of data."[50]

182. By using data ingestion tools, Facebook is able to rapidly translate the information it receives from the Pixel in order to display relevant ads to consumers. For example, if a consumer visits a retailer's webpage and places an item in their shopping cart without purchasing it, the next time the shopper visits Facebook, an ad for that item will appear on the shopper's Facebook page.[51] This evidences that Facebook, in fact, views and categorizes data as they are received from the Pixel.

183. Moreover, even if Facebook eventually deletes or anonymizes Private Information that it receives from Plaintiffs and Class Members, it must first view that information in order to identify it as containing Private Information suitable for removal.

[49] Ankush Sinha Roy, *How Does Facebook Handle The 4+ Petabyte Of Data Generated Per Day? Cambridge Analytica - Facebook Data Scandal*, Medium (Sep 15, 2020), https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4 (last visited July 11, 2023). Facebook employees would not be able to view each piece of data individually – millions of them per second – without the aid of technology. Just as a microscope or telescope allows the user to see very small or very distant objects by zooming in, Facebook's big data management software allows the company to see all of this data at once by zooming out.

[50] Shivang, *Facebook Database [Updated] – A Thorough Insight Into The Databases Used @Facebook*, ScaleYourApp, https://scaleyourapp.com/what-database-does-facebook-use-a-1000-feet-deep-dive/ (last visited July 11, 2023). Facebook uses ODS, Scuba, and Hive to manage its massive data stores. These technologies are not traditional databases; they are specialized databases for big data designed to process data specifically for analysis—"such as [viewing] hidden patterns, correlations, market trends and customer preferences."

[51] David Vranicar, *A Complete Guide To Facebook Tracking For Beginners*, Oberlo (Oct. 4, 2021), https://www.oberlo.com/blog/facebook-pixel (last visited July 11, 2023).

Accordingly, there is a breach of confidentiality the instant the information is disclosed or received without authorization. As described by the HHS Bulletin:

> It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place and requires that there is an applicable Privacy Rule permission for disclosure.[52]

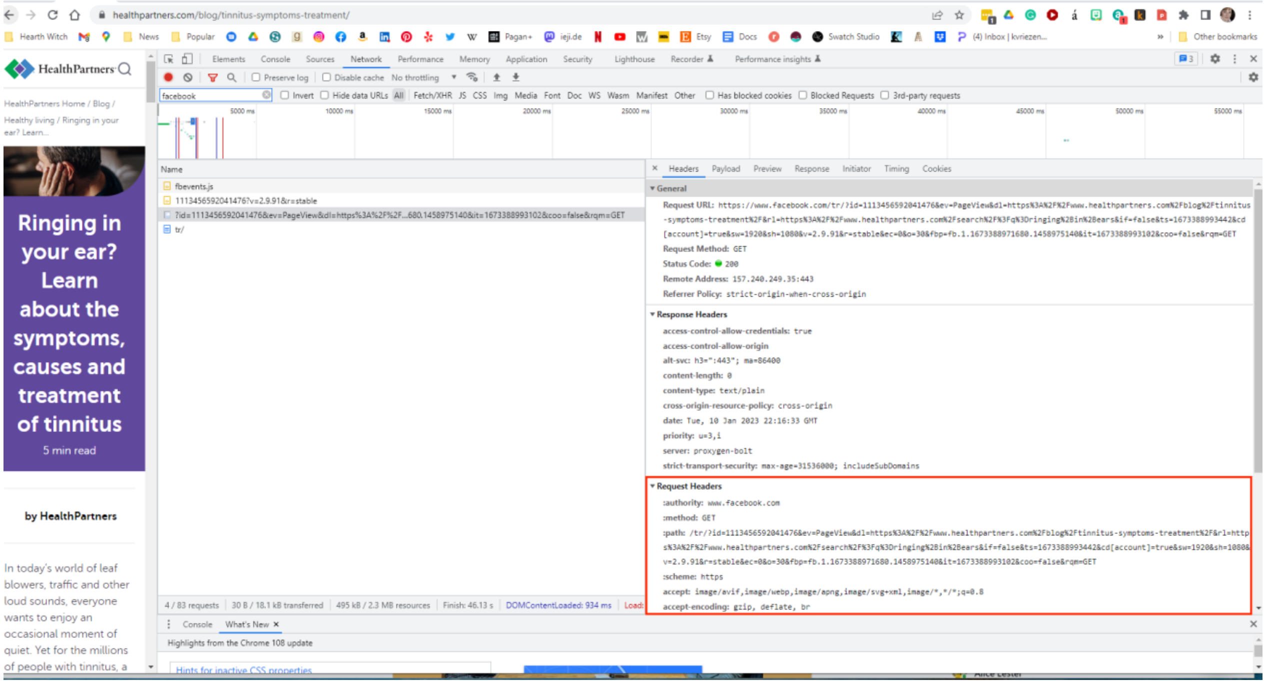
iv. Plaintiff Vriezen Has Specific Evidence of Defendant's Tracking Pixel Communicating With Facebook Regarding Her Private Information.

184. Plaintiff Vriezen submitted medical information to Defendant via the Website. Because Defendant utilizes the Facebook Pixel, the Website's Source Code sends a secret set of instructions back to the individual's browser, causing the Pixel to send Plaintiff Vriezen's FID, the Pixel ID, and the Website's URL to Facebook. For instance, when Plaintiff Vriezen visited Defendant's Website to research medical conditions, the Facebook Pixel reported back Plaintiff Vriezen's FID as well as the Website and other data specified by Defendant secretly to Facebook.

185. For example, on January 10, 2023, Plaintiff Vriezen visited Defendant's Webpage for a specific medical treatment. Upon Plaintiff Vriezen visiting the Website and communicating Private Information to Defendant regarding her medical treatment, the Pixel (i.e., Pixel ID 111345692041476) sent that Private Information to Facebook.

[52] *Supra* n.16.

186. The Pixel sent Plaintiff's data and information from Defendant's Website to Facebook. The screenshot below identifies the following: (1) the Pixel by specific code—111345692041476; (2) Plaintiff's c_user profile, i.e., the FID which identifies her in Facebook by name; and (3) the Facebook Request Header. The Facebook Request Header establishes the Facebook Pixel's transmission of information from Defendant's Website to Facebook.



HealthPartners Home / Blog / Healthy living / Ringing in your ear? Learn...

Ringing in your ear? Learn about the symptoms, causes and treatment of tinnitus

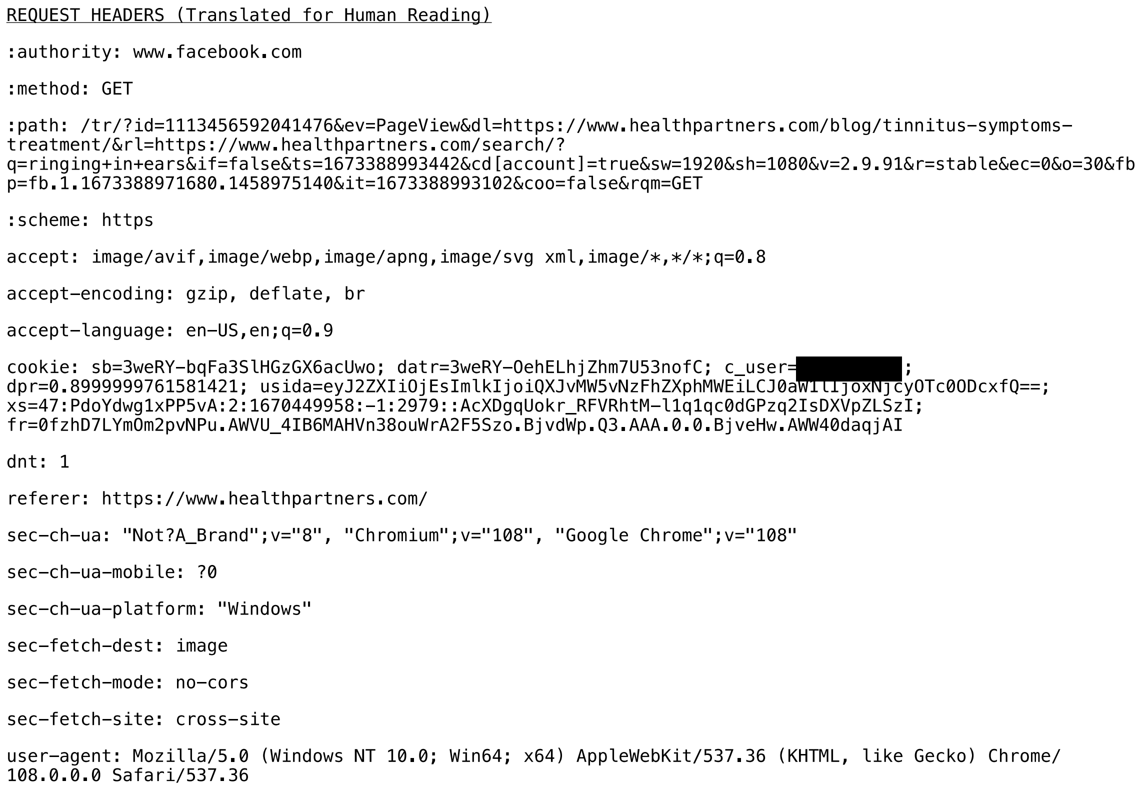
5 min read

by HealthPartners

In today's world of leaf blowers, traffic and other loud sounds, everyone wants to enjoy an occasional moment of quiet. Yet for the millions of people with tinnitus, a

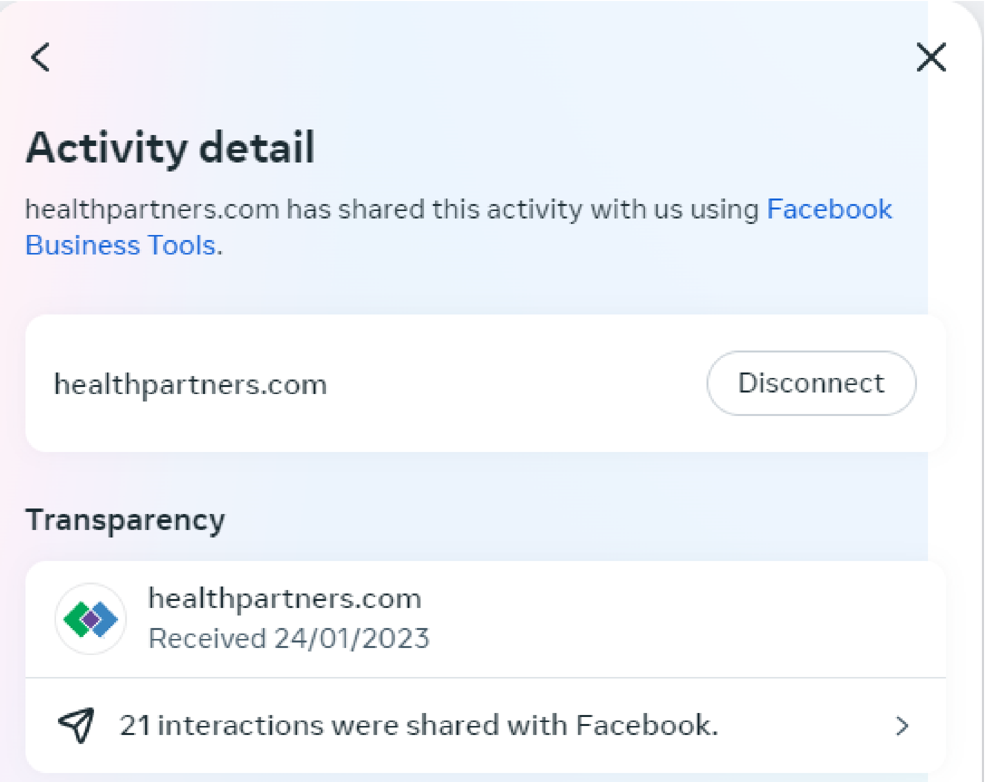
```
fbevents.js
1113456592041476?v=2.9.91&r=stable
?id=1113456592041476&ev=PageView&dl=https%3A%2F%2F...680.1458975140&it=1673388993102&coo=false&rqm=GET
tr/

4 / 83 requests | 30 B / 18.1 kB transferred | 495 kB / 2.3 MB resources | Finish: 46.13 s | DOMContentLoaded: 934 ms | Load:

Highlights from the Chrome 108 update
```

```
▾ General
   Request URL: https://www.facebook.com/tr/?id=1113456592041476&ev=PageView&dl=https%3A%2F%2Fwww.healthpartners.com%2Fblog%2Ftinnitus
   -symptoms-treatment%2F&rl=https%3A%2F%2Fwww.healthpartners.com%2Fsearch%2F%3Fq%3Dringing%2Bin%2Bears&if=false&ts=1673388993442&cd
   [account]=true&sw=1920&sh=1080&v=2.9.91&r=stable&ec=0&o=30&fbp=fb.1.1673388971680.1458975140&it=1673388993102&coo=false&rqm=GET
   Request Method: GET
   Status Code: ● 200
   Remote Address: 157.240.249.35:443
   Referrer Policy: strict-origin-when-cross-origin
▾ Response Headers
   access-control-allow-credentials: true
   access-control-allow-origin
   alt-svc: h3=":443"; ma=86400
   content-length: 0
   content-type: text/plain
   cross-origin-resource-policy: cross-origin
   date: Tue, 10 Jan 2023 22:16:33 GMT
   priority: u=3,i
   server: proxygen-bolt
   strict-transport-security: max-age=31536000; includeSubDomains
▾ Request Headers
   :authority: www.facebook.com
   :method: GET
   :path: /tr/?id=1113456592041476&ev=PageView&dl=https%3A%2F%2Fwww.healthpartners.com%2Fblog%2Ftinnitus-symptoms-treatment%2F&rl=http
   s%3A%2F%2Fwww.healthpartners.com%2Fsearch%2F%3Fq%3Dringing%2Bin%2Bears&if=false&ts=1673388993442&cd[account]=true&sw=1920&sh=1080&
   v=2.9.91&r=stable&ec=0&o=30&fbp=fb.1.1673388971680.1458975140&it=1673388993102&coo=false&rqm=GET
   :scheme: https
   accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
   accept-encoding: gzip, deflate, br
```



```
REQUEST HEADERS (Translated for Human Reading)

:authority: www.facebook.com

:method: GET

:path: /tr/?id=1113456592041476&ev=PageView&dl=https://www.healthpartners.com/blog/tinnitus-symptoms-
treatment/&rl=https://www.healthpartners.com/search/?
q=ringing+in+ears&if=false&ts=1673388993442&cd[account]=true&sw=1920&sh=1080&v=2.9.91&r=stable&ec=0&o=30&fb
p=fb.1.1673388971680.1458975140&it=1673388993102&coo=false&rqm=GET

:scheme: https

accept: image/avif,image/webp,image/apng,image/svg xml,image/*,*/*;q=0.8

accept-encoding: gzip, deflate, br

accept-language: en-US,en;q=0.9

cookie: sb=3weRY-bqFa3SlHGzGX6acUwo; datr=3weRY-OehELhjZhm7U53nofC; c_user=[redacted];
dpr=0.8999999761581421; usida=eyJ2ZXIiOjEsImlkIjoiQXJvMW5vNzFhZXphMWEiLCJ0aW1lIjoxNjcyOTc0ODcxfQ==;
xs=47:PdoYdwg1xPP5vA:2:1670449958:-1:2979::AcXDgqUokr_RFVRhtM-l1q1qc0dGPzq2IsDXVpZLSzI;
fr=0fzhD7LYmOm2pvNPu.AWVU_4IB6MAHVn38ouWrA2F5Szo.BjvdWp.Q3.AAA.0.0.BjveHw.AWW40daqjAI

dnt: 1

referer: https://www.healthpartners.com/

sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108", "Google Chrome";v="108"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

sec-fetch-dest: image

sec-fetch-mode: no-cors

sec-fetch-site: cross-site

user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
108.0.0.0 Safari/537.36
```

187. Additionally, Plaintiff Vriezen’s Facebook records show the Pixel sent her private communications with Defendant to Facebook on multiple occasions:



Activity detail

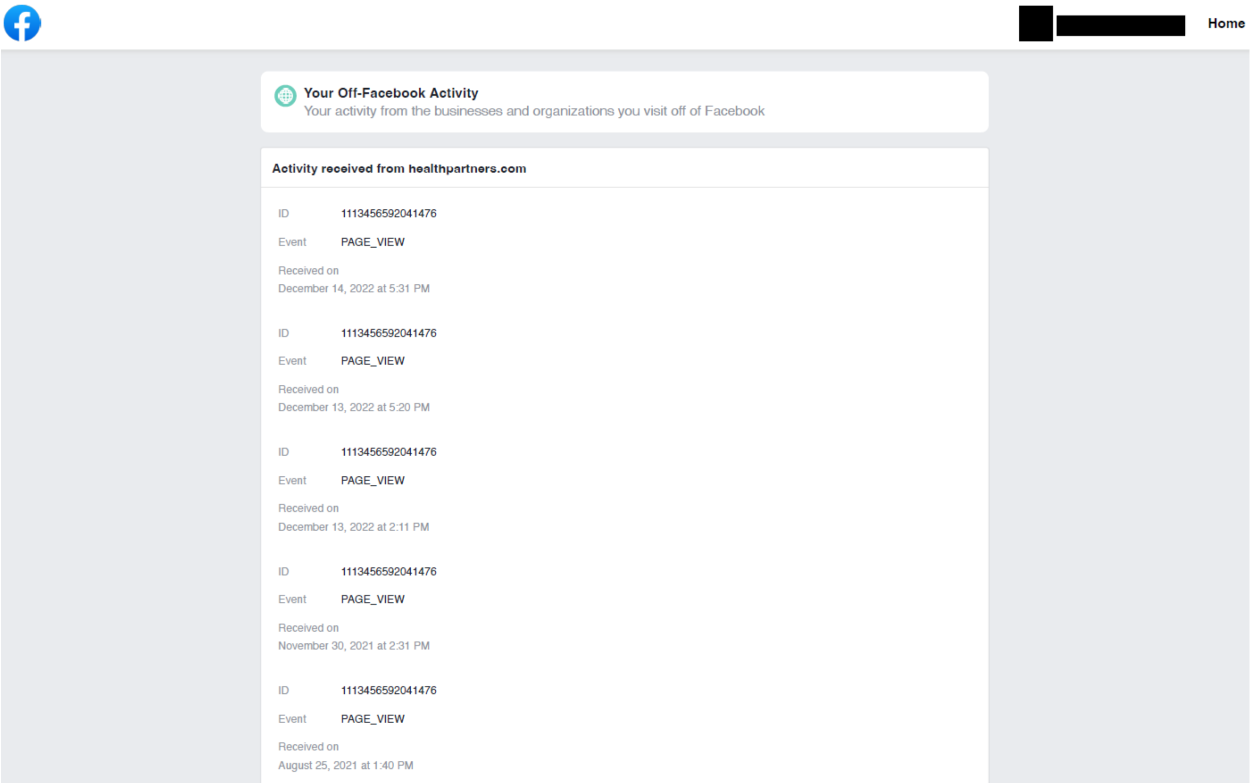
healthpartners.com has shared this activity with us using Facebook Business Tools.

healthpartners.com

Transparency

healthpartners.com
Received 24/01/2023

21 interactions were shared with Facebook.



[redacted]

Your Off-Facebook Activity
Your activity from the businesses and organizations you visit off of Facebook

Activity received from healthpartners.com

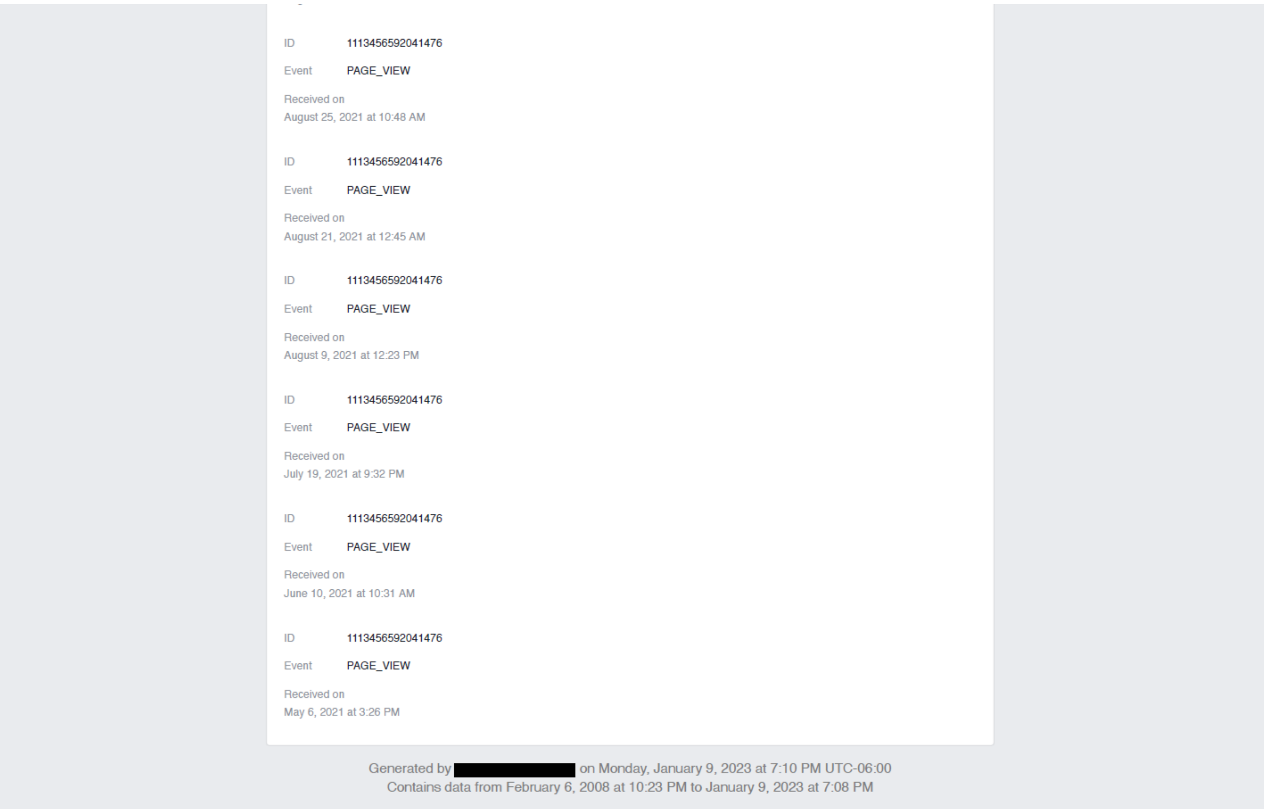
ID 1113456592041476
Event PAGE_VIEW
Received on
December 14, 2022 at 5:31 PM

ID 1113456592041476
Event PAGE_VIEW
Received on
December 13, 2022 at 5:20 PM

ID 1113456592041476
Event PAGE_VIEW
Received on
December 13, 2022 at 2:11 PM

ID 1113456592041476
Event PAGE_VIEW
Received on
November 30, 2021 at 2:31 PM

ID 1113456592041476
Event PAGE_VIEW
Received on
August 25, 2021 at 1:40 PM



ID 1113456592041476

Event PAGE_VIEW

Received on
August 25, 2021 at 10:48 AM

ID 1113456592041476

Event PAGE_VIEW

Received on
August 21, 2021 at 12:45 AM

ID 1113456592041476

Event PAGE_VIEW

Received on
August 9, 2021 at 12:23 PM

ID 1113456592041476

Event PAGE_VIEW

Received on
July 19, 2021 at 9:32 PM

ID 1113456592041476

Event PAGE_VIEW

Received on
June 10, 2021 at 10:31 AM

ID 1113456592041476

Event PAGE_VIEW

Received on
May 6, 2021 at 3:26 PM

Generated by [redacted] on Monday, January 9, 2023 at 7:10 PM UTC-06:00
Contains data from February 6, 2008 at 10:23 PM to January 9, 2023 at 7:08 PM

188. Indeed, as the screenshots above demonstrate, Plaintiff Vriezen's communications with Defendant, and the Private Information contained in those communications, were transmitted to Facebook via Defendant's Pixel, with the first recorded transmission occurring May 6, 2021.

189. Upon downloading her offsite activity from www.Facebook.com, Plaintiff Vriezen learned that Defendant's Pixel transmitted her communications on Defendant's Website on the following dates: May 6, 2021; June 10, 2021; July 19, 2021; August 9, 2021; August 2, 2021; August 25, 2021 (2x); November 30, 2021; December 13, 2022 (2x); and December 14, 2022.

190. On these dates and times, Plaintiff Vriezen remembers seeking medical treatment and/or browsing Defendant's website for medical treatment or care. For example, on May 6, 2021, and June 10, 2021, Plaintiff Vriezen sought and has records of the medical services and treatment she received from Defendant.

191. Plaintiff Vriezen's Facebook records confirm the Pixel on Defendant's Website surreptitiously transmitted Plaintiff Vriezen's communications on Defendant's Website on specific dates and times Plaintiff Vriezen sought medical treatment from Defendant—her healthcare provider—via Defendant's Website.

C. Defendant's Conduct is Unlawful and Violates its Patients' Rights.

i. Defendant's Conduct Violates its Own Privacy Policies and Promises

192. Defendant's privacy policies represent to Plaintiffs and Class Members that Defendant will keep Private Information private and confidential and they will only disclose Private Information under certain circumstances.[53]

193. Defendant publishes several privacy policies that represent to patients and Website visitors that Defendant will keep sensitive information confidential and will only disclose Private Information under certain circumstances, none of which apply here.

[53] *Notice of Privacy Practices*, HealthPartners (effective Nov. 17, 2018), https://www.healthpartners.com/ucm/groups/public/@hp/@public/documents/documents/cntrb_009405.pdf (last visited: July 11, 2023).

194. Defendant's Notice of Privacy Practices explains Defendant's legal duties with respect to Private Information and the exceptions for when Defendant can lawfully use and disclose Plaintiffs' and Class Members' Private Information in the following ways:

- Follow the law;
- Help with public health and safety issues;
- Respond to organ and tissue donation requests;
- Work with a medical examiner or funeral director
- Handle workers' compensation;
- Respond to lawsuits and legal actions; and
- With your written permission.

195. Defendant's Privacy Policy does not permit Defendant to intercept, transmit, and/or disclose Plaintiffs' and Class Members' Private Information to third parties, including Facebook, for marketing purposes.

196. Defendant's Privacy Policy acknowledges Defendant is required by law to maintain the confidentiality of Plaintiffs' and Class Members' Private Information, subject to the exceptions listed above.[54]

197. Defendant violated its own Privacy Policy by unlawfully intercepting and disclosing Plaintiffs' and Class Members' Private Information to Facebook and third parties without adequately disclosing that it shares Private Information with third parties

[54] *Id.*

and without acquiring the specific patients' consent or authorization to share the Private Information.

ii. Defendant Violated HIPAA Standards

198. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[55]

199. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

200. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[56]

201. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

[55] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

[56] *Supra* n.16.

202. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

203. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

a. Names;

***

H. Medical record numbers;

***

J. Account numbers;

***

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

> O. Internet Protocol (IP) address numbers; … and
>
> R. Any other unique identifying number, characteristic, or code…; and"
>
> The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

204. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

205. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

206. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

207. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

208. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[57]

209. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover,

[57] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. Dept. of Health & Hum. Servs. (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited July 11, 2023).

> *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[58]

210. As alleged above, an HHS Bulletin highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[59]

211. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

212. Defendant's actions violated HIPAA Rules per this Bulletin.

iii. Defendant Violated Industry Standards

213. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

214. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

215. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

216. AMA Code of Medical Ethics Opinion 3.2.4 provides:

[58] *Marketing*, U.S. Dept. of Health & Hum. Servs. (Revised April 3, 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited July 11, 2023)

[59] *See supra* n.16.

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (A) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

217. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…: (c) release patient information only in keeping ethics guidelines for confidentiality.

D. Plaintiffs' and Class Members' Expectation of Privacy

218. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

219. Indeed, at all times when Plaintiffs and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

E. IP Addresses are Personally Identifiable Information

220. On information and belief, through the use of the Facebook Pixel on the Defendant's Website, Defendant also disclosed and otherwise assisted Facebook with intercepting Plaintiffs' and Class Members' Computer IP addresses.

221. An IP address is a number that identifies the address of a device connected to the Internet.

222. IP addresses are used to identify and route communications on the Internet.

223. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

224. Facebook tracks every IP address ever associated with a Facebook user.

225. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

226. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

227. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

F. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures

228. The primary motivation and a determining factor in Defendant's interception and disclosure of Plaintiffs' and Class Members' Private Information was to commit wrongful and tortious acts in violation of federal and state laws as alleged here, namely, the use of patient data for advertising in the absence of express written consent. Defendant's further use of the Private Information after the initial interception and disclosure for marketing and revenue generation was in violation of HIPAA and an invasion of privacy. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook in the form of enhanced advertising services and more cost-efficient marketing on its platform.

229. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

230. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients to get more patients to use its services. Defendant did so through use of the intercepted patient data it obtained, procured, and/or disclosed in the absence of express written consent.

231. By utilizing the Pixel, the cost of advertising and retargeting was reduced through further use of the unlawfully intercepted and disclosed Private Information, thereby benefitting Defendant while invading the privacy of Plaintiffs and Class Members and violating their rights under federal and Minnesota law.

G. Plaintiffs' and Class Members' Private Information Had Financial Value

232. Plaintiffs' and Class Members' data and Private Information have economic value. Facebook regularly uses data that it acquires to create Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

233. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure will keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

234. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[60]

235. Similarly, CNBC published an article in 2019, observing that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[61]

[60] *See* Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, Time (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/ (last visited July 11, 2023).

[61] *See* Christina Farr, *Hospital Execs Say They Are Getting Flooded With Requests For Your Health Data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited July 11, 2023).

TOLLING

236. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Until information became publicly available regarding healthcare providers use of the Pixel, Plaintiffs did not know (and had no reasonable way of knowing) that their Private Information was intercepted and unlawfully disclosed to Facebook because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

237. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

238. The Nationwide Class that Plaintiffs seeks to represent is defined as follows:

> **All individuals residing in the United States who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website, and had their Private Information disclosed to a third party without authorization.**

239. In addition to the claims asserted on behalf of the National Class, Plaintiffs assert claims on behalf of a separate sub-class (the "Minnesota Subclass"), defined as follows:

> **All individuals residing in Minnesota who are, or were, patients of Defendant or any of its affiliates, used Defendant's Website, and had their Private Information disclosed to a third party without authorization.**

240. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer

or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

241. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

242. Numerosity, Fed R. Civ. P. 23(a)(1). The National Class and Minnesota Subclass members are so numerous that joinder of all members is impracticable. Upon information and belief, there are over one million individuals whose Private Information may have been improperly disclosed to Facebook, and the National Class and Minnesota Subclass members are identifiable within Defendant's records.

243. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing the Private Information of Plaintiffs and Class Members to Facebook and/or additional third parties;

d. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

f. Whether Defendant adequately addressed and fixed the practices that permitted the unlawful disclosure of patient Private Information;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

h. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

i. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

j. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices; and

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Defendant's disclosure of their Private Information.

244. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because they all had their Private Information compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

245. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs and counsel intend to prosecute this action vigorously.

246. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged in this Complaint; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

247. Policies Generally Applicable to the Class. Fed. R. Civ. P. 23(b)(2). This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged in this Complaint apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

248. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

249. The litigation of the claims is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

250. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

251. Unless a class-wide injunction is issued, Defendant may continue disclosing the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of in this Complaint, and Defendant may continue to act unlawfully as set forth in this Complaint.

252. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

253. Issue Certification, Fed. R. Civ. P. 23(c)(4). Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests here. Such particular issues include, but are not limited to, the following:

a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information with respect to Defendant's privacy policy;

c. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties;

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

254. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

<u>COUNT I</u>
VIOLATION OF THE MINNESOTA HEALTH RECORDS ACT
(Minn. Stat. § 144.291, *et seq*.)
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

255. Plaintiffs repeat and re-allege each and every allegation contained in the Consolidated Complaint as if fully set forth here.

256. Under the Minnesota Health Records Act, "health record" means any information, whether oral or recorded in any form or medium that relates to the past,

present, or future physical or mental health or condition of a patient; the provision of healthcare to a patient; or the past, present, or future payment of provision of healthcare to a patient. Minn. Stat. § 144.291, subd. 2(c) (the "MHRA").

257. The Private Information of Plaintiffs and Class Members that was surreptitiously recorded and transmitted to Facebook via Defendant's Pixel and CAPI falls within the definition of "Health Records" as that term is defined by the MHRA.

258. Plaintiffs and Class Members are "patients" as that term is defined under the MHRA at all times relevant under Minn. Stat. §144.291, subd. 2(g).

259. Under the MHRA, it is unlawful for a third party to access a patient's health records from a provider, or a person who receives records from a provider, without the patient or the patient's legally authorized representative's consent, specific authorization in law, or a representative from a provider that holds a signed and dated consent from the patient authorizing the release. Minn. Stat. § 144.293, subd. 2(1-3).

260. Through the Pixel and CAPI, Defendant released Plaintiffs' and Class Members' health records to Facebook.

261. Neither Plaintiffs nor Class Members consented to have their records released via the Pixel or CAPI.

262. Defendant's installation of the Pixel and CAPI on its Website constitutes an "affirmative" release under Minnesota law. *See Larson v. Nw. Mut. Ins. Co.*, 855 N.W.2d 293, 302 (Minn. 2014).

263. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently or intentionally releasing the health record is liable to the patient for compensatory damages, plus costs and reasonable attorneys' fees. Minn. Stat. § 144.298, subd. 2.

264. Plaintiffs have suffered compensatory damages including, but not limited to, invasion of their privacy, loss of value of their Private Information, directed harassing and spam Facebook advertisements, and the mental and emotional anguish caused by Defendant's surreptitious recording and transmittal of their Private Information, including medical diagnoses, to Facebook.

265. As a result of Defendant's violations of the MHRA, Plaintiffs and Class Members seek all damages authorized by law, including compensatory damages, costs, and attorneys' fees.

COUNT II
INVASION OF PRIVACY
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

266. Plaintiffs repeat and re-allege each and every allegation contained in the Consolidated Complaint as if fully set forth here.

267. The Private Information of Plaintiffs and Class Members consist of private and confidential facts and information that were never intended to be shared beyond private communications.

268. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

269. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

270. Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information to Facebook, a third-party social media and marketing giant, is highly offensive to a reasonable person.

271. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' Private Information constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

272. Defendant's conduct constitutes an intentional physical or sensory intrusion on Plaintiffs' and Class Members' privacy because Defendant facilitated Facebook's simultaneous collection and exploitation of confidential communications.

273. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when it installed the Pixel onto its Website because the purpose of the Pixel is to track and disseminate individual's communications with the Website for the purpose of marketing and advertising.

274. Because Defendant intentionally and willfully incorporated the Facebook Pixel into its Website and encouraged patients to use that Website for healthcare purposes,

Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class Members.

275. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and Class Members was disclosed to a third party without authorization, causing Plaintiffs and the Class to suffer damages.

276. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, plus prejudgment interest, and costs.

277. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendant and still in the possession of Facebook and the wrongful disclosure of the information cannot be undone.

278. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook who on information and belief continues to possess and utilize that information.

279. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further intruding into the privacy and

confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

280. Plaintiffs repeat and re-allege each and every allegation contained in the Consolidated Complaint as if fully set forth here.

281. As a condition of utilizing Defendant's Website and receiving services from Defendant's healthcare facilities and professionals, Plaintiffs and Class Members provided their Private Information and compensation for their medical care.

282. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

283. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

284. Plaintiffs and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

285. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information without consent to third parties like Facebook.

286. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged in this Complaint, including, but not limited to, the loss of the benefit of their bargain and diminution in value of Private Information.

287. Plaintiffs and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

288. Plaintiffs repeat and re-allege each and every allegation contained in the Consolidated Complaint as if fully set forth here.

289. Defendant benefits from the use of Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at their expense.

290. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

291. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

292. The benefits that Defendant derived from Plaintiffs and Class Members was not offered by Plaintiffs and Class Members gratuitously and rightly belongs to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in Minnesota and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

293. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

294. Plaintiffs repeat and re-allege each and every allegation contained in the Consolidated Complaint as if fully set forth here.

295. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became a guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of disclosure of their Private Information to unauthorized third parties; and (3) to maintain complete and accurate records of what patient information (and where) Defendant did and does store and disclose.

296. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep private and not disclose the Private Information of its patients.

297. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to keep their Private Information confidential and by disclosing it to third parties.

298. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic Private Information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

299. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

300. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4).

301. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members violation of 45 C.F.R. § 164.308(b) by failing to obtain satisfactory assurances, including in writing, that its business associates and/or subcontractors would appropriately safeguard Plaintiffs' and Class Members' Private Information.

302. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

303. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network in violation of 45 C.F.R. § 164.312(e)(1).

304. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing Private Information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq*.

305. Defendant breached its duties owed to Plaintiffs and Class Members by failing to keep Private Information confidential as required by the MHRA, Minn. Stat. § 144.291, *et seq*.

306. Defendant breached its duties owed to Plaintiffs and Class Members by failing to keep Private Information confidential as required by Minnesota's Patient Bill of Rights, Minn. Stat. § 144.651 subd. 16.

307. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including

independent contractors) on the policies and procedures with respect to Private Information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security Private Information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

308. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

309. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, as described above.

COUNT VI
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

310. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth here.

311. Medical providers have a duty to their patient to keep their patients' Private Information completely confidential. *See* Minn. Stat. § 144.651 subd. 15-16; Minn. Stat. § 144.293.

312. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

313. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant installed its Pixel and CAPI to disclose and transmit to third

parties Plaintiffs' and Class Members' communications with Defendant, including Private Information and the contents of such information.

314. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

315. The third-party recipients included, but may not be limited to, Facebook.

316. The harm arising from a breach of provider-patient confidentiality includes mental suffering due to the exposure of private information and erosion of the essential confidential relationship between the healthcare provider and the patient.

317. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. Plaintiffs and Class Members have suffered general damages for invasion of their rights in an amount to be determined by a jury;

e. Plaintiffs and Class Members are entitled to nominal damages for each independent violation;

f. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;

g. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

h. Defendant's actions diminished the value of Plaintiffs' and Class Members' Private Information; and

i. Defendant's actions violated the property rights Plaintiffs and Class Members have in their Private Information.

COUNT VII
NEGLIGENCE
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

318. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth here.

319. Medical providers have a duty to their patient to keep their patients' Private Information completely confidential. *See* Minn. Stat. § 144.651 subd. 15-16; Minn. Stat. § 144.293.

320. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website.

321. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant negligently installed the Pixel and CAPI to disclose and transmit to third parties Plaintiffs' and Class Members' communications with Defendant, including Private Information and the contents of such information.

322. These disclosures were made without Plaintiffs' or Class Members' knowledge, consent, or authorization, and were unprivileged.

323. The third-party recipients included, but may not be limited to, Facebook.

324. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class Members were damaged by Defendant's breach in that:

a. Private Information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Plaintiffs and Class Members face ongoing harassment and embarrassment in the form of unwanted targeted advertisements;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. Plaintiffs and Class Members have suffered general and compensatory damages that were proximately caused by Defendant's negligence, in an amount to be determined by a jury;

e. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without compensation for such data;

f. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

g. Defendant's negligent actions diminished the value of Plaintiffs' and Class Members' Private Information; and

COUNT VIII
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq.*
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

325. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth here.

326. The ECPA protects both sending and receipt of communications.

327. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

328. The transmissions of Plaintiffs' Private Information to Defendant via Defendant's Website qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

329. The transmissions of Plaintiffs' Private Information to the Virtuwell Webpage and medical professionals qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(2).

330. **Electronic Communications**. The transmission of Private Information between Plaintiffs and Class Members and Defendant via its Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

331. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

332. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

333. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel deployed by Defendant to effectuate the sending and acquisition of patient communications.

334. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Pixel imbedded and run on its Website, contemporaneously and intentionally disclosed, and endeavored to disclose, the contents of Plaintiffs' and Class Members' electronic communications to third parties, including Facebook, without authorization or consent and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c).

335. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the Pixel imbedded and run on its Website, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiffs' and Class Members' electronic communications, for purposes other than providing health care services to Plaintiffs and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

336. Whenever Plaintiffs and Class Members interacted with Defendant's Website, Defendant, through the source code it imbedded and ran on its web properties, contemporaneously and intentionally redirected the contents of Plaintiffs' and Class

Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook.

337. Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiffs' and Class Members' regarding Private Information, including, but not limited to, symptoms, medical conditions, physician lookup, treatment, medication, and scheduling.

338. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

339. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

340. Defendant intentionally used the wire or electronic communications for its own business purposes, unrelated to the transactions between Plaintiffs, Class members and Defendant. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' Private Information for its own gain.

341. Defendant was not acting under color of law to intercept Plaintiffs' and Class Members' wire or electronic communication.

342. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code and/or CAPI.

343. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

344. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, violations of the Minnesota's Patient Bill of Rights, the MHRA, and invasion of privacy, among others.

345. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

346. Defendant is a "party to the communication" with respect to patient communications. However, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

347. Defendant's acquisition of patient communications that were used and disclosed to Facebook was done for purposes of committing criminal and tortious acts in violation of the laws of the United States and Minnesota, including:

a. Criminal violation of HIPAA, 42 U.S.C. § 1320d-6;

b. Criminal violation of Minnesota's Unauthorized Computer Access statute (Minn. Stat. § 609.891);

c. Violation of the Minnesota's Patient's Bill of Rights, Minn. Stat. § 144.651, subd. 16;

d. Violation of MHRA, Minn. Stat. § 144.291, *et seq.*;

e. Violation of the Minnesota Unfair Deceptive Trade Practices Act ("MUDPTA") Minn. Stat. § 235D.43-48; and

f. Invasion of Privacy.

348. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

349. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

350. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it:

a. Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and

b. Disclosed individually identifiable health information to Facebook without patient authorization.

351. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

352. Under Minn. Stat. § 609.891, a person commits the offense of unauthorized computer access if the person intentionally and without authorization attempts to or does penetrate a computer security system or electronic terminal.

353. Defendant violated Minn. Stat. § 609.981 when its Pixel penetrated Plaintiffs' and Class Members' web browser, without their consent, and transmitted their Private Information to Facebook.

354. Under Minnesota's Health Care Bill of Rights, Minn. Stat. § 144.651 subd. 15-16, patients have a right to privacy as it relates to their personal and medical care and shall be assured confidential treatment of their personal and medical records.

355. Defendant violated the Minnesota's Patient's Bill of Rights by disclosing Plaintiffs' and Class Members' Private Information to third parties without authorization or consent.

356. Under MHRA, Minn. Stat. § 144.291, *et seq*., all medical records must be treated as confidential. A hospital must receive written authorization of a patient for release of medical information outside the hospital.

357. Defendant violated the MHRA by failing to treat Plaintiffs' and Class Members' medical records as confidential and by disclosing those records to third parties outside the hospital without written authorization or consent and without an authorized appropriate purpose. Increasing Defendant's revenues through enhanced marketing and advertising and online targeting is not an appropriate authorized purpose.

358. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their individually-identifiable patient health information on its Website, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' individually-identifiable patient health information with Facebook, third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know were receiving their individually-identifiable patient health information, and that Plaintiffs and Class Members did not consent to receive this information.

359. Defendant accessed, obtained, and disclosed Plaintiffs' and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

360. As such, Defendant cannot viably claim any exception to ECPA liability.

361. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually identifiable patient health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiffs and Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiffs' and Class Members' individually identifiable patient health information without providing any value or benefit to Plaintiffs or Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and Class Members' individually identifiable patient health information, such as understanding how people use its Website and determining what ads people see on its Website, without providing any value or benefit to Plaintiffs or Class Members;

d. Defendant has failed to provide Plaintiffs and Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information; and

e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, test results, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

362. As a result of Defendant's violation of the ECPA, Plaintiffs are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory damages, and attorneys' fees and costs.

COUNT IX
MINNESOTA UNIFORM DECEPTIVE TRADE PRACTIECE ACT ("MUDPTA")
Minn. Stat. §325D.43-48
(On Behalf of Plaintiffs, the Nationwide Class and the Minnesota Subclass)

363. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth here.

364. The MDUPTA prohibits deceptive trade practices in person's business, vocation, or occupation. *See* Minn. Stat. § 325D.44, subd. 1.

365. Defendant advertised, offered, or sold goods or services in Minnesota and therefore engaged in business directly or indirectly affecting the people of Minnesota, Defendant violated Minn. Stat. § 325D.44, including, but not limited to, the following provisions: (a) represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and (b) engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

366. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the MDUPTA, including, but not limited to, the following: (1) promising to protect Plaintiffs' and Class Members' Private Information via its Privacy Policies and then, in fact, knowingly, transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook; (2) unlawfully disclosing Plaintiffs' and Class Members' Private Information to Facebook; (3) failing to disclose or omitting material facts that that Plaintiffs' and Class Members' Private Information would be disclosed to third parties; (4) failing to obtain Plaintiffs' and Class Members' consent in transmitting Plaintiffs' and Class Members' Private Information to Facebook; and (5) knowingly violating industry and legal standards regarding the protection of Plaintiffs' and Class Members' Private Information.

367. These actions also constitute deceptive and unfair acts or practices because Defendant knew its Website contained the Pixel and CAPI and also knew the Pixel and CAPI would be unknown and/or not easily discoverable by Plaintiffs and Class Members.

368. Defendant intended that Plaintiffs and Class Members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

369. Had Defendant disclosed to Plaintiffs and Class Members that its Website was transmitting Private Information to Facebook via the Pixel and CAPI, Plaintiffs and the Class Members would not have provided their Private Information to Defendant.

370. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Minnesota Class. Plaintiffs and the Minnesota Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

371. As a result of Defendant's wrongful conduct, Plaintiffs and Class Members were injured in that they never would have provided their Private Information to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their Private Information from being taken and misused by others.

372. As a direct and proximate result of Defendant's violations of the MDUPTA, Plaintiffs and Class Members have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiffs and Class Members would not have made had they known of Defendant's inadequate data security; lost control over the value of their Private Information; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Private Information, entitling them to damages in an amount to be proven at trial.

373. Pursuant to MDUPTA, Plaintiffs and the Class are entitled to injunctive relief and other appropriate relief, as alleged.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs and counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:

D. For an award of compensatory damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Respectfully submitted,

/s/ Bryan L. Bleichner
Bryan L. Bleichner (MN #0326689)
Jeffrey D. Bores (MN #227699)
Philip J. Krzeski (MN #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Gary M. Klinger (admitted *pro hac vice*)
Alexandra M. Honeycutt*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
ahoneycutt@milberg.com

Interim Co-Lead Counsel for Plaintiffs

Terence R. Coates (admitted *pro hac vice*)
Dylan J. Gould (admitted *pro hac vice*)
MARKOVITS, STOCK & DEMARCO,
LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 4502
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon (admitted *pro hac vice*)
LYON LAW FIRM
2754 Erie Ave.
Cincinnati, Ohio 45208
Phone: (513) 381-2333

Fax: (513) 766-9011
jlyon@thelyonfirm.com

David S. Almeida (admitted *pro hac vice*)
ALMEIDA LAW GROUP
849 Webster Ave.
Chicago, Illinois 60614
Phone: (312) 576-3024
david@alameidalawgroup.com

Stephen R. Basser (admitted *pro hac vice*)
Samuel M. Ward* (admitted *pro hac vice*)
BARRACK RODOS & BACINE
One America Plaza
600 West Broadway, Suite 900
San Diego, California 92101
Phone: (619) 230-0800
Fax: (619) 230-1874
sbasser@barrack.com
sward@barrack.com

John Emerson (admitted *pro hac vice*)
EMERSON FIRM LLP
2500 Wilcrest, Ste. 300
Dallas, Texas 77042
Phone: (800) 551-8649
Fax: (501) 286-4659
jemerson@emersonfirm.com

Brian C. Gudmundson (#336695)
Jason P. Johnston (#0391206)
Michael J. Laird (#398436)
Rachel K. Tack (#0399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Hart L. Robinovitch (#0240515)
ZIMMERMAN REED LLP
14646 N. Kierland Blvd., Suite 145
Scottsdale, AZ 85254
Telephone: (480) 348-6400
hart.robinovitch@zimmreed.com

Daniel E. Gustafson (#202241)
Karla M. Gluek (#238399)
David A. Goodwin (#386715)
Anthony J. Stauber (#401093)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
dgustafson@gustafsongluek.com
kgluek@gustafsongluek.com
dgoodwin@gustafsongluek.com
tstauber@gustafsongluek.com

* *pro hac vice applications forthcoming*